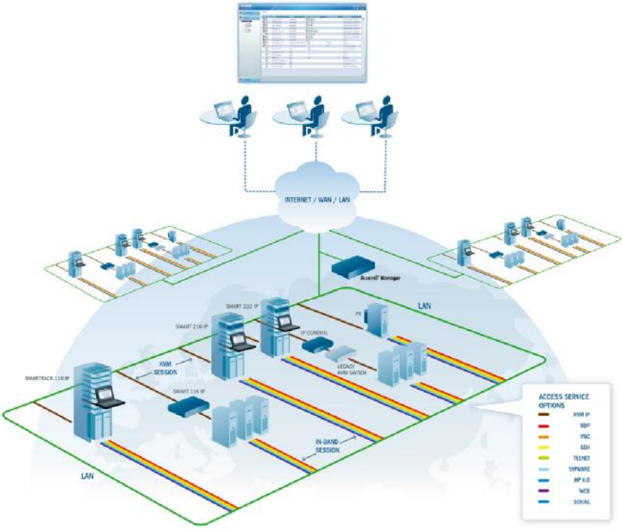
MINICOM
advanced systems

AccessIT

User Guide



w w w . m i n i c o m . c o m

International HQ

Jerusalem, Israel
Tel: + 972 2 535 9666
minicom@minicom.com

America

Linden, NJ, USA
Tel: + 1 908 486 2100
info.usa@minicom.com

Technical support - support@minicom.com

5UM70173 V1 6/09

About this User Guide

This User Guide provides installation and operation instructions for the AccessIT Manager system produced by Minicom Advanced Systems. It is intended for system administrators and network managers, and assumes that readers have general understanding of networks, LDAP, hardware and software.

All information in this User Guide is subject to change without prior notice.

User Guide Feedback

Your feedback is very important to help us improve our documentation. Please email any comments to: ug.comments@minicom.com

Please include the following information: Guide name, part number and version number (as appears on the front cover).

Copyright

Copyright © 2009 Minicom Advanced Systems Ltd.

All marks are trademarks or registered trademarks of their respective owners.

Table of Contents

1. Introduction

AccessIT is an appliance based application that provides IT staff with secure and centralized management of all remote access services in the organization. It operates in both Windows and Linux environments and is accessible from Internet Explorer and Firefox.

AccessIT is a web-based management solution that consolidates in-band and out-of-band remote access services onto one user-friendly web portal. It provides a unified point and click view of all IT assets together with their assigned remote access services. AccessIT is a single sign-in solution making it simple and easy for IT staff to enter the system regardless of their location at any given moment.

AccessIT manages remote access to up to 250 mission-critical IT and network devices of the business whether they are inside the server room or distributed around the organization or branch offices. These can include: servers, virtual servers, IP-enabled KVM switches, routers, firewalls, serial console servers, network switches, printers, power distribution units (PDUs), environmental devices (sensors), surveillance IP cameras and more.

AccessIT provides unique seamless (one-click) access to IT assets through a select, predefined list of Access Services™ that include: RDP, VNC, VMware ESX Server, VMware Server 1x and 2x, SSH, Telnet, HP iLO and KVM (Minicom or 3rd party). You can also customize any other remote access method in a few simple steps.

1.1 Key features

IT Management - AccessIT centralizes the management of all devices, authentication and global operation from a Web browser. The local administrator can monitor, control and manage the various devices, user accounts and authorization from one Web interface.

Automatic Discovery - Minicom IP devices are discovered automatically by the AccessIT Manager.

Access Services - Connect to a variety of both hardware and software external resources such as: ILO, RDP, SSH, VNC and web pages etc, from the AccessIT interface.

Security - AccessIT provides a secure environment, adhering to the most stringent industry standards.

Availability - Maximizes uptime by centralizing management and allowing immediate and effective maintenance.

Virtual Media - Virtual Media is a very useful tool for those who need to manage large numbers of computers such as commercial IT data center managers. A Target computer can be made to boot to one of many virtual disks that can perform any variety of tasks such as virus scans of the Target's physical drive or patch management or even complete installation of the operating system on a Target computer.

1.2 System components

The AccessIT Manager system comes with the following:

- AccessIT Manager appliance
- Rack mounting kit

1.3 Terminology

Below are some terms and their meanings used in this guide.

Term	Meaning
Targets	Computers/servers and other services e.g. printers, firewalls, PDUs etc. that are accessed remotely via the AccessIT.
Client computer	The PC running a remote AccessIT session
Remote session	The process of accessing and controlling Targets connected to a KVM/IP device from a Client computer

1.4 System diagram

The diagram below gives a brief outline of the AccessIT system setup. Section 3 on page 12 explains the system setup in more detail.

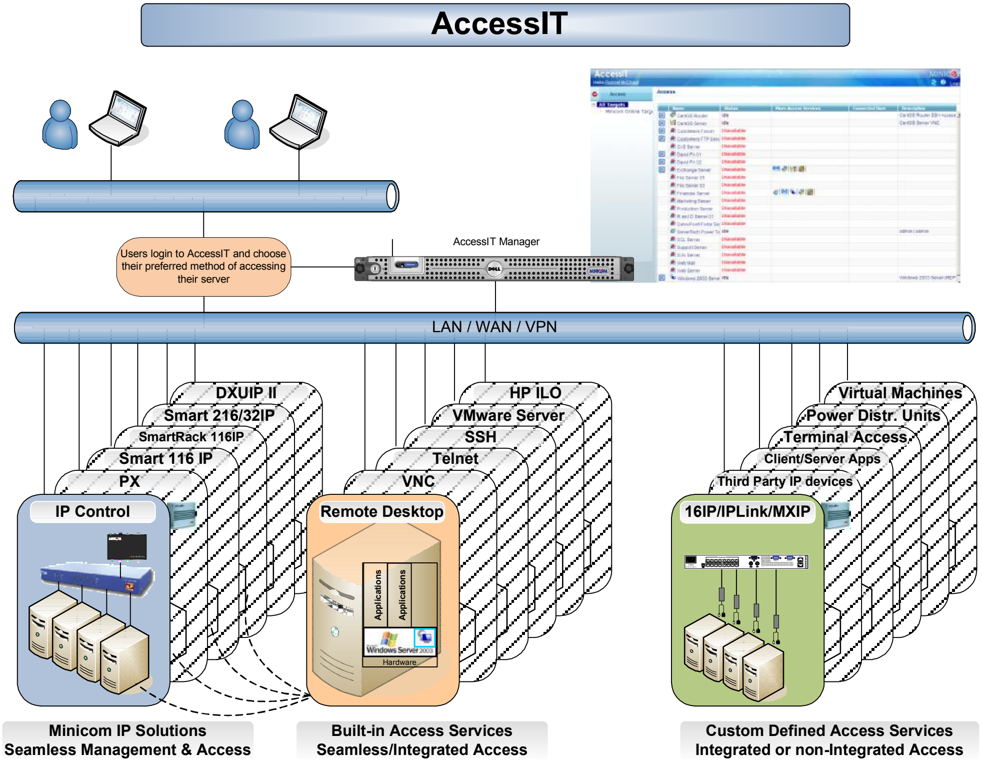


Figure 1 System diagram

2. Pre-installation guidelines

Prepare a list of all AccessIT system components. You will need this information to configure the system.

Appendix A on page 134 contains 2 lists of the details you need to prepare for Minicom KVM/IP devices and PX units (not PX Serial). Photocopy or print out Appendix A. For other access services see section 2.1 below.

The lists should include the IP device name and MAC address, KVM switch and the Target details.

For each Target, list:

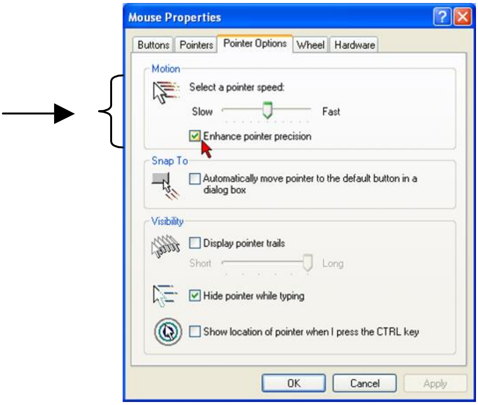
- A unique and clearly identifiable name
- The operating system
- Non-default mouse settings. Default mouse settings do not need to be listed

Note! For Windows XP and later

(Relevant to all IP devices except PX USB)

For Windows XP and later deactivate **Enhanced pointer precision**. To do so:

From the **Control Panel** select **Printers and Other Hardware.** Click the **Mouse** icon. The Mouse Properties box appears. See Figure 2. Select the **Pointer Options** tab.



Motion

Select a pointer speed:

Slow — Fast

☑ Enhance pointer precision

Snap To

□ Automatically move pointer to the default button in a dialog box

Visibility

□ Display pointer trails

Short — Long

☑ Hide pointer while typing

□ Show location of pointer when I press the CTRL key

Figure 2 Pointer tab

The **Motion** section slider bar must be in the center, and the **Enhanced pointer precision** checkbox must be unchecked. Click OK to save changes.

2.1 Access services details

Besides the Minicom KVM/IP devices mentioned above, you can connect to Targets via the following Access services through AccessIT:

- Minicom’s PX Serial
- Web
- ILO
- RDP
- SSH
- VNC
- Telnet
- VMware Server

These services are elaborated on in the section 3.6.

All service applications must be installed on the local (client) computers.

See section 10.3 on page 55 which sets out the details required for each of the above Access service.

2.1.1 Adding user defined Access services

You can also add your own access services, explained on page 65.

3. Understanding the system – an overview

The figure below shows a typical AccessIT application.

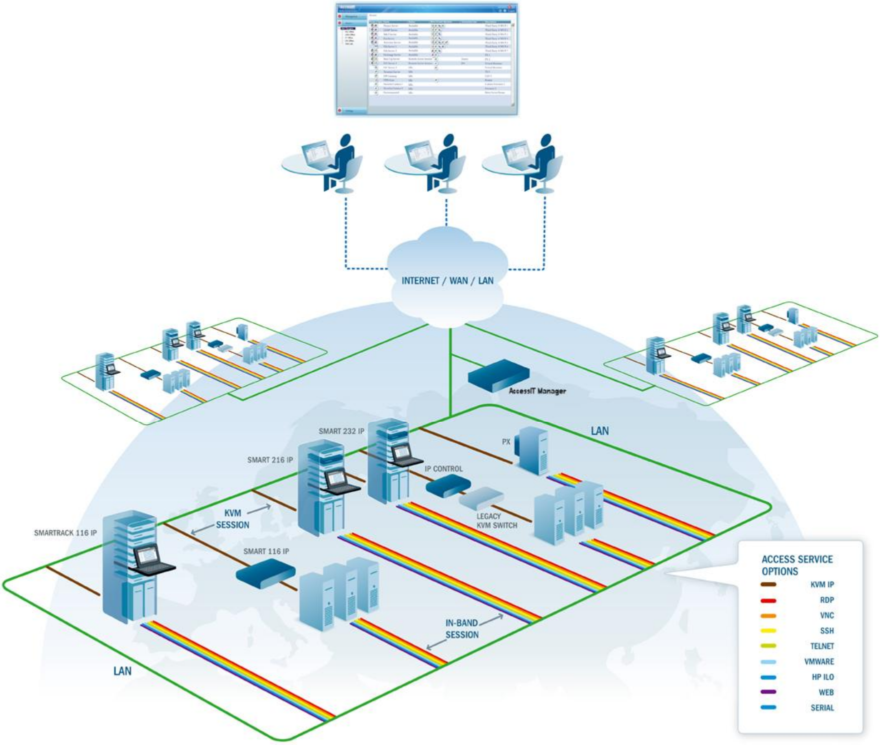


Figure 3 AccessIT typical application

The system works as follows:

Data centers in locations throughout the world are connected to Minicom IP devices and to other 3rd party access services. The Minicom IP devices are Centralized Management enabled allowing AccessIT to access/control the Targets connected to all IP devices via IP.

Users access the AccessIT web interface and depending on their level of access permissions can access and control the Targets.

3.1 Creating users

An Administrator can create users with 2 different possible permission types:

- Administrator
- User

These permission types are explained fully in section 6. In the example below 4 users are created with various permission types.

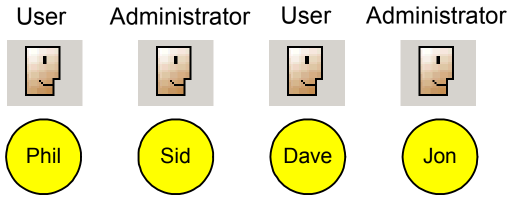


Figure 4 Users with different permissions

Once an Administrator creates Targets or sets of Targets (explained below) in the system, users can be assigned access to individual Targets or sets of Targets.

3.2 Forming users into Groups

You can form users into Groups. In the example below 3 users are formed into the Finance group. Note! Groups can contain users with different levels of user permissions.

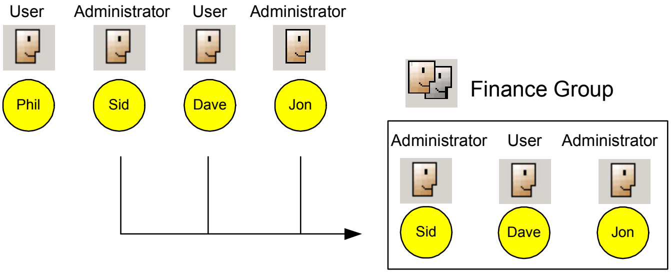


Figure 5 Forming users into groups

3.3 Creating Targets

An Administrator creates Targets corresponding to the physical servers connected to the IP devices, explained in section 7, and also to Targets corresponding to e.g. printers, firewalls, PDUs and IDSs etc accessed via Access Services™ - see page 15. In the example below, four Targets are created and given identifying names. They can be named by location, server type or operating system or any other unique feature associated with that particular server.

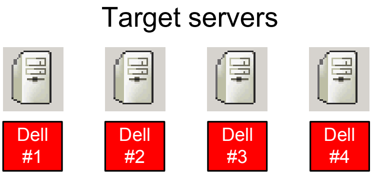


Figure 6 Created Targets

3.4 Forming Targets into sets

Targets can be formed into sets. You can for example create a set of all financial servers. In the example below 3 Targets are formed into Target Set - Finance.

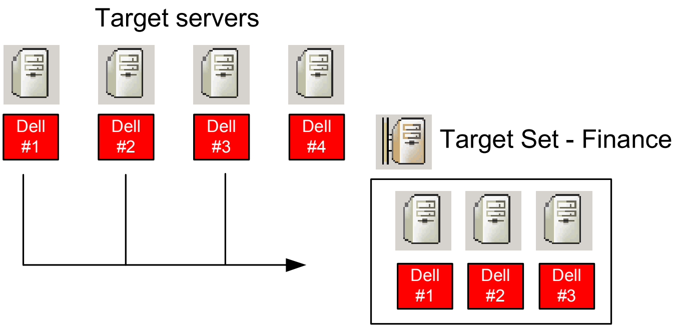


Figure 7 Forming Targets into sets

3.5 Associating a User Group with a Target Set

You can then associate the User Group with the Target Set, thus giving access rights to all the Targets in the Set to all members of the Group.

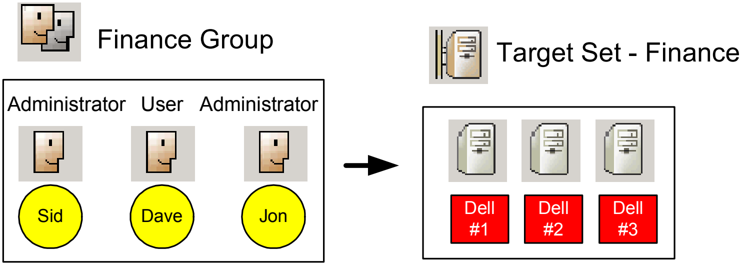


Figure 8 User Group - Target Set association

In the example above the Finance Group is associated with the Target Set – Finance.

This means that:

- The Finance Group has access rights to Target Set - Finance.
- Any user added to the Finance Group will automatically have access rights to Target Set - Finance.

Note! Users can be members of many different groups. In the example below Sid belongs to the Finance Group and also to the Marketing Group.

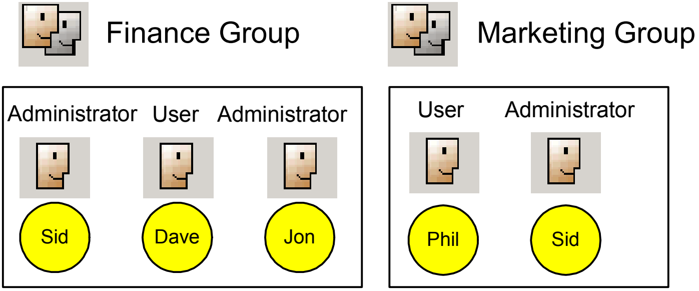


Figure 9 Same user in different Groups

The Marketing Group could be associated with Targets or Target Sets that the Finance Group is not. Sid being a member of both Groups has access to Targets both Groups are associated with. Phil only has access to Targets associated with the Marketing Group. Dave and Jon only have access to Targets associated with the Finance Group.

3.6 Access services

The Access Services™ feature supports a wide range of remote access technologies. This enables the assignment of multiple services to a single Target, so you have the option of in-band or out-of-band access to the same device.

KVM/IP is a hardware method of accessing and controlling a Target. The other Access Services encompass gaining remote access and control of a Target through the internet or LAN network via Minicom's PX Serial or 3rd party software. Both hardware and software methods of access are managed by AccessIT.

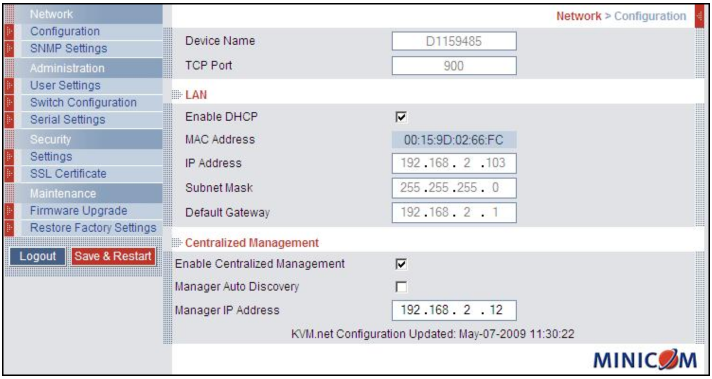
AccessIT also enables you to effortlessly integrate any new remote access technology into the remote access portal.

Besides the Minicom KVM/IP devices, you can connect to Targets via the following Access services through AccessIT:

- Minicom's PX Serial - PX Serial is a one-port RS232/422/485 to Redundant Ethernet device server.
- Web – Browser based web service
- ILO - HP Integrated Lights-Out (iLO). HP ILO gives seamless access to HP servers.
- RDP - Remote Desktop Protocol. RDP is a multi-channel protocol that allows a user to connect to a computer running Microsoft Terminal Services.
- SSH - Secure Shell. SSH is a network protocol that allows data to be exchanged using a secure channel between two computers. An SSH client program is typically used for establishing connections to an SSH daemon.
- VNC - Virtual Network Computing. VNC is a graphical desktop sharing system which uses the RFB protocol. VNC is platform-independent — a VNC viewer on any operating system usually connects to a VNC server on any other operating system. There are clients and servers for almost all GUI operating systems.
- Telnet - **TEL**ecommunication **NET**work. TELNET is a network protocol used on the Internet or LAN connections.
- VMware Server - VMware Server is a free virtualization product for Windows and Linux servers with enterprise-class support. It enables companies to partition a physical server into multiple virtual machines and to start experiencing the benefits of virtualization. VMware Server gives seamless access to virtual machines.

4. Setting up the system

Set up the Minicom IP device systems according to their User Guide instructions. In order to be managed by AccessIT, all Minicom IP devices must be configured to be Centralized Management enabled. This is done from the Network Configuration page of each IP device. For example, see the Centralized Management section in Figure 10, Centralized Management is enabled by selecting the **Enable Centralized Management** checkbox.



Device Name D1159485
TCP Port 900

LAN

Enable DHCP ☑
MAC Address 00:15:9D:02:66:FC
IP Address 192 .168 . 2 .103
Subnet Mask 255 .255 .255 . 0
Default Gateway 192 .168 . 2 . 1

Centralized Management

Enable Centralized Management ☑
Manager Auto Discovery ☐
Manager IP Address 192 .168 . 2 . 12

KVM.net Configuration Updated: May-07-2009 11:30:22

Figure 10 Network Configuration page sample

Also in the Centralized Management section in Figure 10, specify how the AccessIT Manager detects the IP device. This can be done either by:

Manager Auto Discovery – when checked, AccessIT automatically detects the IP device if it resides on the same network segment.

Manager IP – If the IP device resides on a different segment, type the static IP address of the AccessIT Manager. (We advise typing the static IP address of the AccessIT Manager even if the IP device resides on the same network segment as the AccessIT Manager).

Install 3rd party access services in all client workstations according to their own installation and configuration instructions. See section 10.3 on page 55 for details required for the integration of the Access services into the AccessIT system.

4.1 Connecting the AccessIT Manager

1. Connect the AccessIT Manager to the network as follows: On the rear panel connect an Ethernet cable to LAN 1. Connect the other end of the Ethernet cable to the network switch.

2. Connect the AccessIT Manager to a power supply outlet.

4.2 AccessIT Manager’s default IP address

Each AccessIT Manager unit comes with the following default values:

IP address - 192.168.1.250.

Subnet mask - 255.255.255.0

Gateway - 192.168.1.1

If these values are not suitable for your network, follow the steps in the section below to display the AccessIT interface. You can then change the IP address of the AccessIT Manager in the **Network** tab under **Settings/Unit Maintenance**, see section 16.2 on page 106.

4.2.1 Changing the AccessIT Manager network parameters

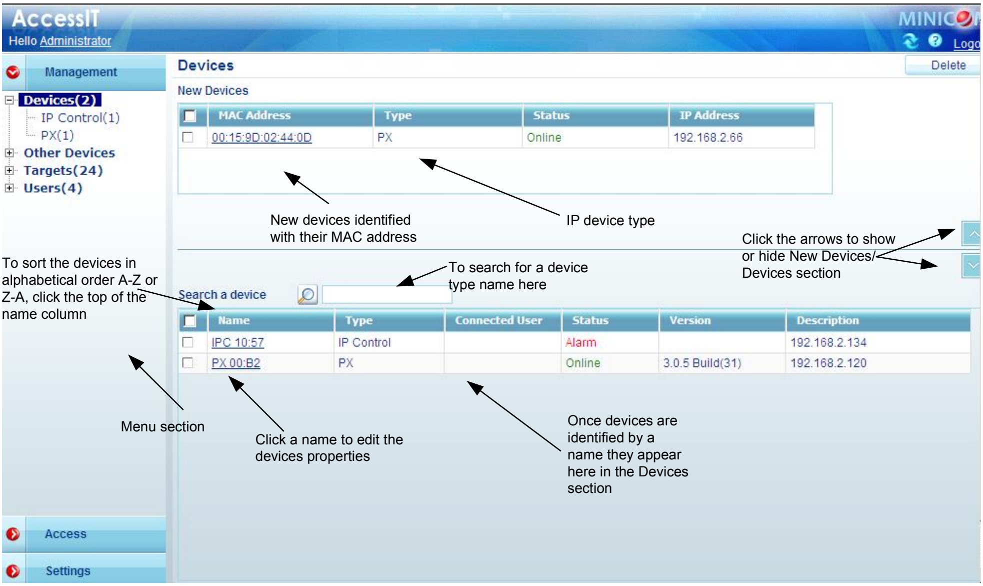
1. Open your Web browser (Internet Explorer version 6.0 - Firefox 3 or higher versions).
2. Type in the IP address of the AccessIT Manager (default IP address https://192.168.1.250) and press **Enter**. (Change your computer network settings, if necessary). The Login page appears.
3. Type the login name **admin** and password **access**.
4. Navigate to the **Network** tab under **Settings/Unit Maintenance** and change the network parameters to suit your network configuration.
5. Press Save and restart the AccessIT Manager.
6. Wait for the system to restart and login with the new IP address.

5. Displaying the AccessIT web interface

To display the Web interface:

1. Open your Web browser (Internet Explorer version 6.0 or Firefox 3 or higher) versions.
2. Type in the IP address of the AccessIT Manager (default IP address https://192.168.1.250) and press **Enter**.

   Note! The IP address must begin with https:// and not http://. The Login page appears. Bookmark it for easy reference.
3. Type the login name and password. Default username is **admin** and password is **access**.
4. Press **Enter**. The Web interface appears, see Figure 11**.**



New Devices

☐	MAC Address	Type	Status	IP Address
☐	00:15:9D:02:44:0D	PX	Online	192.168.2.66

☐	Name	Type	Connected User	Status	Version	Description
☐	IPC 10:57	IP Control		Alarm		192.168.2.134
☐	PX 00:B2	PX		Online	3.0.5 Build(31)	192.168.2.120

New devices identified with their MAC address

IP device type

Click the arrows to show or hide New Devices/ Devices section

To sort the devices in alphabetical order A-Z or Z-A, click the top of the name column

To search for a device type name here

Menu section

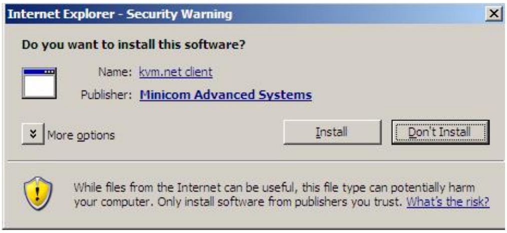
Click a name to edit the devices properties

Once devices are identified by a name they appear here in the Devices section

Figure 11 Devices page

Note! On first connection the AccessIT GUI prompts you to install the AccessIT client software, see Figure 12. Click **Install**.

Note! In Firefox, the client plugin is installed when you navigate to the Access section.



Internet Explorer - Security Warning

Do you want to install this software?

Name: kvm.net client

Publisher: Minicom Advanced Systems

While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

Figure 12 AccessIT client

5.1 Menu section

The menu section on the left, see Figure 11 is sub-divided into 3 sections:

Management, which includes the configuration pages for IP devices, PDUs, Serial Console servers, Targets and Users/Groups.

Access, which contains access pages to all allowed Targets and Target Groups.

Settings which contains 3 configuration sections: Application, Attached Devices and Maintenance.

This Guide explains the menu sections from the point of view of first setting up the system and then operating it.

So the guide explains in the following order how to:

- Create Users
- Configure Targets
- Configure Devices
- Configure Other Devices
- Configure Settings
- Configure Access Services
- Access the system
- Configure Advanced settings

6. Creating users

There are two possible methods of inputting users into the system. When using local authentication (see page 55) users and groups are created in the AccessIT GUI. When using an LDAP authentication server (see page 81) users and groups are imported from a Windows Active Directory. With both authentication methods, an Administrator can grant users different access permissions as follows:

Administrator - An Administrator can view, modify, manage and control all AccessIT Manager configuration settings, including creating new users.

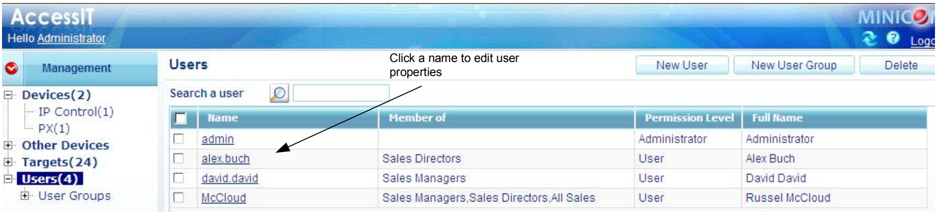
User – A User cannot access or change any of the AccessIT Manager configuration settings. When a User logs in, only the Targets that the user has permission to access appear.

With local authentication, once you have created users you can form them into Groups, making management changes easier by e.g. adding or deleting permitted Targets per Group rather than per individual user. Creating Groups is explained in section 6.5 on page 25.

In LDAP mode go to section 6.1 below.

To create a new user (in local authentication mode):

1. From the **Management** menu, select **Users**. The **Users** page appears showing the default Administrator (admin) at the top of the list, see Figure 13.



Click a name to edit user properties

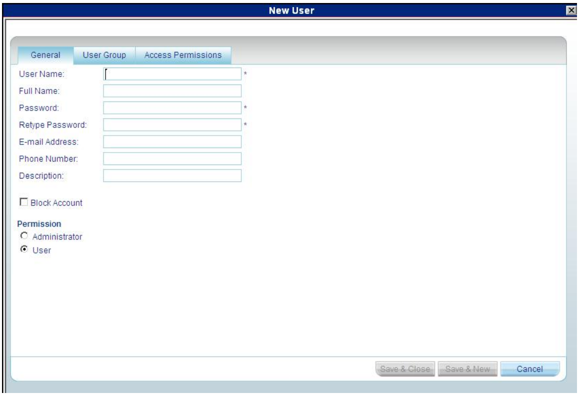
☐	Name	Member of	Permission Level	Full Name
☐	admin		Administrator	Administrator
☐	alex.buch	Sales Directors	User	Alex Buch
☐	david.david	Sales Managers	User	David David
☐	McCloud	Sales Managers,Sales Directors,All Sales	User	Russel McCloud

Figure 13 Users page

The columns show the following:

- **Name** – User's login name. You can search for a user by typing the login name in the Search a user field. You can sort the names out in alphabetical order A-Z or Z-A by clicking the top of the Name column.
- **Member of** – groups the user is a member of.
- **Permission Level** – Administrator or User. You can sort the users out in Permission Level order - Administrators then Users or Users then Administrators - by clicking the top of the Permission Level column.
- **Full Name** – Full User name.

2. Click New User. The following appears.



New User

General | User Group | Access Permissions

User Name: *

Full Name:

Password: *

Retype Password: *

E-mail Address:

Phone Number:

Description:

☐ Block Account

Permission

○ Administrator

● User

Save & Close | Save & New | Cancel

Figure 14 New User

6.1 General tab

Fill in the following details:

User name - type a login name. A User name cannot be identical to any other existing User name. It can contain uppercase or lowercase characters except for the following:

: ; ? & < > ”

A User name cannot include spaces.

Full Name - type the User’s real name

Password / **Retype Password** - type a password.

E-mail address, Phone number, Description – these are optional fields.

Block Account - To prevent a user from entering the system, select the Block Account checkbox. To re-enable the account, unselect the checkbox.

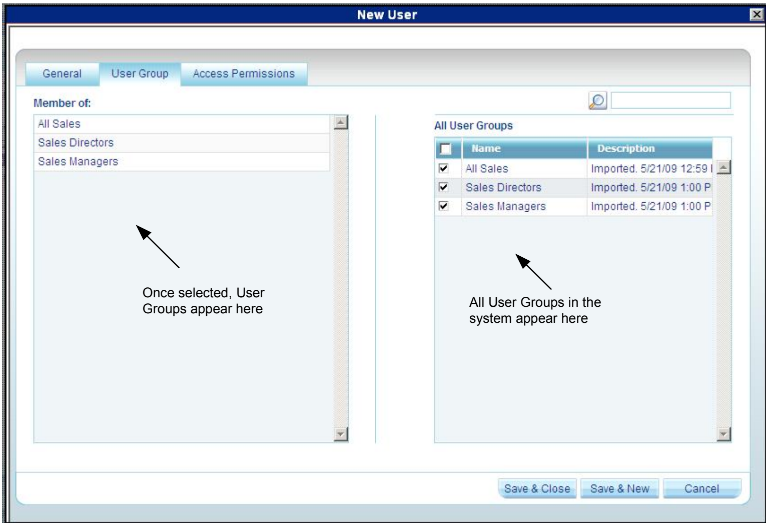
Permission – select the account type as outlined above on page 21.

6.2 User Group tab

Once you have created users you can put them into existing Groups. This gives users the access rights of that User Group. Section 6.5 on page 25 explains how to create a User Group.

To add a User to an existing User Group or Groups:

1. Press the **Users Group** tab, Figure 15 appears. All existing Groups appear in the **All User Groups** list.



Member of:

- All Sales
- Sales Directors
- Sales Managers

Once selected, User Groups appear here

All User Groups

☐	Name	Description
☑	All Sales	Imported. 5/21/09 12:59 I
☑	Sales Directors	Imported. 5/21/09 1:00 P
☑	Sales Managers	Imported. 5/21/09 1:00 P

All User Groups in the system appear here

Figure 15 User Group tab

2. Select the Groups that the new User will be a member of. The Groups appear in the **Member of** list.

6.2.1 Removing Users from a Group

To remove Users from a Group:

In the **All User Groups** section, unselect the Group's checkbox. The Group is removed from the **Member of** list.

6.3 Access Permissions tab

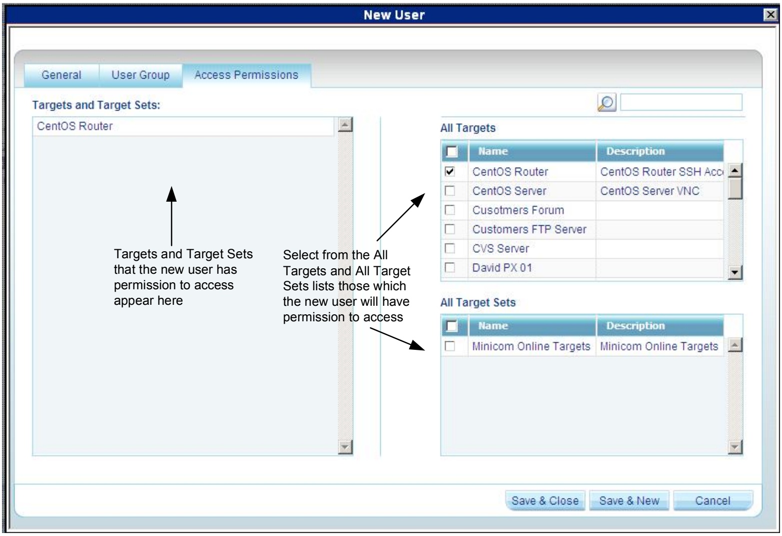
You can choose which Targets and Target sets the user has permission to access.

Notes:

- A User can have access to a Target as an individual User or as a Group member.
- A User or Group of Users can be associated with several Target Sets.
- When a User logs into the AccessIT web interface he sees only Targets and Target Sets that he has been associated with. See section 18 on page 124.

To choose which Targets / Target Sets the user will have access to:

1. Press the **Access Permissions** tab. The following appears.



Targets and Target Sets:

CentOS Router

Targets and Target Sets that the new user has permission to access appear here

Select from the All Targets and All Target Sets lists those which the new user will have permission to access

All Targets

☐	Name	Description
☑	CentOS Router	CentOS Router SSH Acc
☐	CentOS Server	CentOS Server VNC
☐	Cusotmers Forum	
☐	Customers FTP Server	
☐	CVS Server	
☐	David PX 01	

All Target Sets

☐	Name	Description
☐	Minicom Online Targets	Minicom Online Targets

Figure 16 Access Permissions tab

The **All Targets** and **All Target Sets** lists show the Targets and All Target sets in the system.

2. Select the checkboxes of the desired Targets / Target sets. They appear in the **Targets** and **Target Sets**: list.

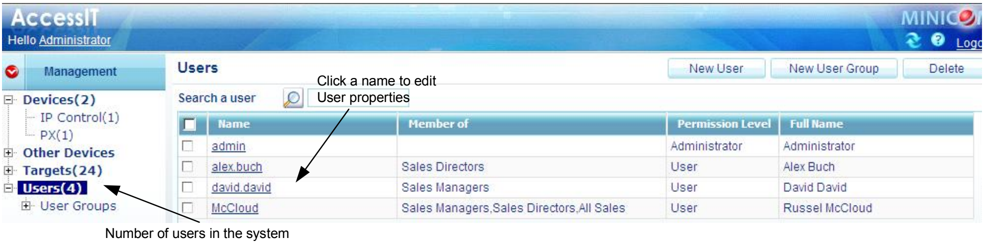
To disassociate a User/Group from a Target:

Unselect the Targets / Target Sets checkbox from the relevant list.

6.4 Saving a user

Click Save & New. The user's details are now in the system.

Repeat this process to add more users. When finished, click Save & Close. All users appear on the Users page. The number of users appears in brackets after Users in the menu, see Figure 17. User Groups appear as a sub-folder in the menu. Creating user groups is explained below.



Click a name to edit User properties

☐	Name	Member of	Permission Level	Full Name
☐	admin		Administrator	Administrator
☐	alex.buch	Sales Directors	User	Alex Buch
☐	david.david	Sales Managers	User	David David
☐	McCloud	Sales Managers,Sales Directors,All Sales	User	Russel McCloud

Number of users in the system

Figure 17 Users in the system

By clicking a user name, an Administrator can access the **General**, **User Group** and **Access Permissions** tabs of this user and change any of the parameters.

6.4.1 Deleting a user

Deleting a user, instantly removes the user's authorization from the AccessIT system and all IP devices.

To delete a user:

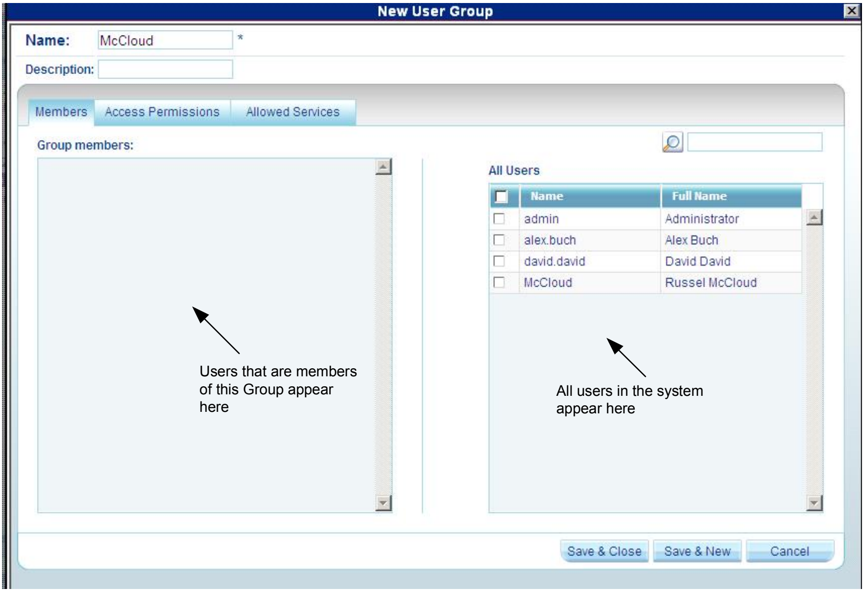
1. On the **Users** page select the checkboxes of the users to be deleted.
2. Press Delete. The user is removed. Press □ to select or deselect all checkboxes with one click.

6.5 Creating a User Group

Once you have created users you can form them into Groups. You then give the same access permissions to the entire group without having to go through the process for each individual user.

To create a User group:

1. From the menu, click **Users** or **User Groups**. On either of these pages, click New User Group. The **New User Group** page appears, see Figure 18.



Name: McCloud *

Description:

Group members:

All Users

□	Name	Full Name
□	admin	Administrator
□	alex.buch	Alex Buch
□	david.david	David David
□	McCloud	Russel McCloud

Users that are members of this Group appear here

All users in the system appear here

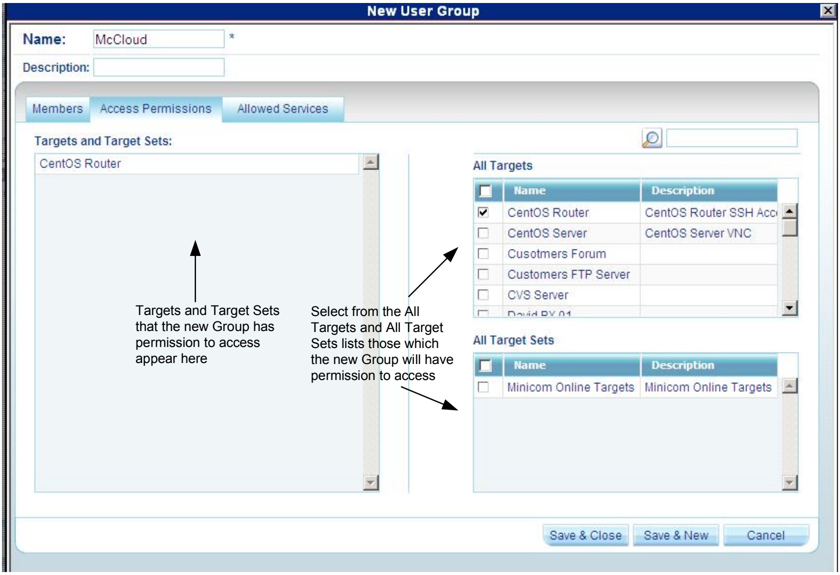
Figure 18 New User Group - Members tab

2. **Name:** Type a unique name for the Group. You can add a description.
3. Select the checkboxes of the users to be part of the Group. They appear in the **Group members** list.

You can access the User Properties page by clicking a user name in the **Group members** list.

6.5.1 Access Permissions tab

Click the **Access Permissions** tab, Figure 19 appears.



New User Group

Name: McCloud *

Description:

Targets and Target Sets:

CentOS Router

All Targets

☐	Name	Description
☑	CentOS Router	CentOS Router SSH Acc
☐	CentOS Server	CentOS Server VNC
☐	Cusotmers Forum	
☐	Customers FTP Server	
☐	CVS Server	
☐	David PX 01	

All Target Sets

☐	Name	Description
☐	Minicom Online Targets	Minicom Online Targets

Targets and Target Sets that the new Group has permission to access appear here

Select from the All Targets and All Target Sets lists those which the new Group will have permission to access

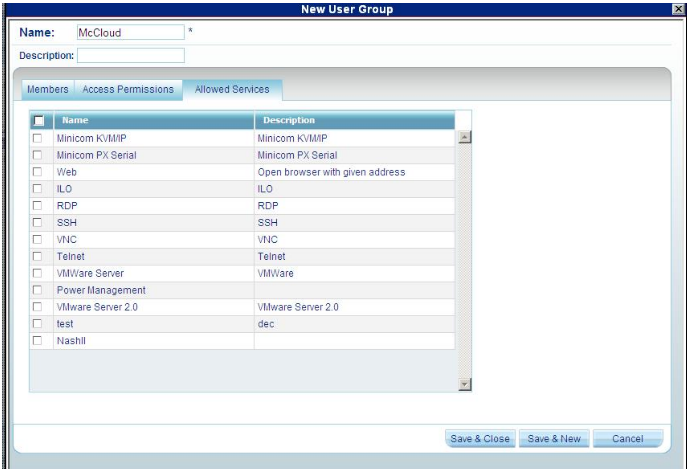
Figure 19 Access Permissions tab

From the **All Targets** and **All Target Sets** lists select the checkboxes of those which the new User Group will have permission to access. When selected the Target/Set appears in the Targets and Target Sets list.

To remove **Targets/Sets**, unselect the checkboxes.

6.5.2 Allowed Services tab

Click the Allowed Services tab. The following appears.



New User Group

Name: McCloud *

Description:

Members | Access Permissions | Allowed Services

□	Name	Description
□	Minicom KVM/IP	Minicom KVM/IP
□	Minicom PX Serial	Minicom PX Serial
□	Web	Open browser with given address
□	ILO	ILO
□	RDP	RDP
□	SSH	SSH
□	VNC	VNC
□	Telnet	Telnet
□	VMWare Server	VMWare
□	Power Management	
□	VMware Server 2.0	VMware Server 2.0
□	test	dec
□	Nashll	

Figure 20 Allowed Services tab

Here you assign Access Services to Group members. If a Group member has permission to access a Target, but there are no assigned Access Services for the Group, then the Group member will not be able to access the Target.

Select the checkboxes of all access services allowed to this Group.

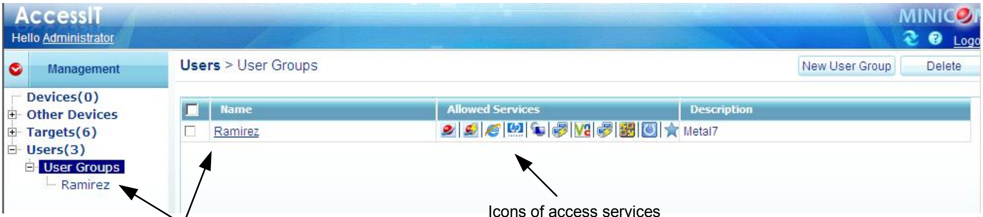
6.5.3 Saving the new Group

Click Save & New. The Group’s details are now in the system.

Repeat this process to add more Groups. When finished, click Save & Close. All Groups appear on the **User** Groups page, see Figure 21.

Tip! The allowed services appear as icons. To see which service the icon represents, hold the mouse over the icon and a tooltip appears with the name of the service.

You can create different access profiles. You can give permission to Targets and define different access rights through the **Allowed Services**.



☐	Name	Allowed Services	Description
☐	Ramirez		Metal7

User Groups

Icons of access services allowed appear here

Figure 21 User Groups page

6.5.4 Deleting a User Group

To delete a Group:

1. On the **Users Group** page select the checkboxes of the Groups to be deleted.

2. Press Delete. The Groups are removed. Press ☐ to select or deselect all checkboxes with one click.

Note: Deleting a Group will not delete the individual users.

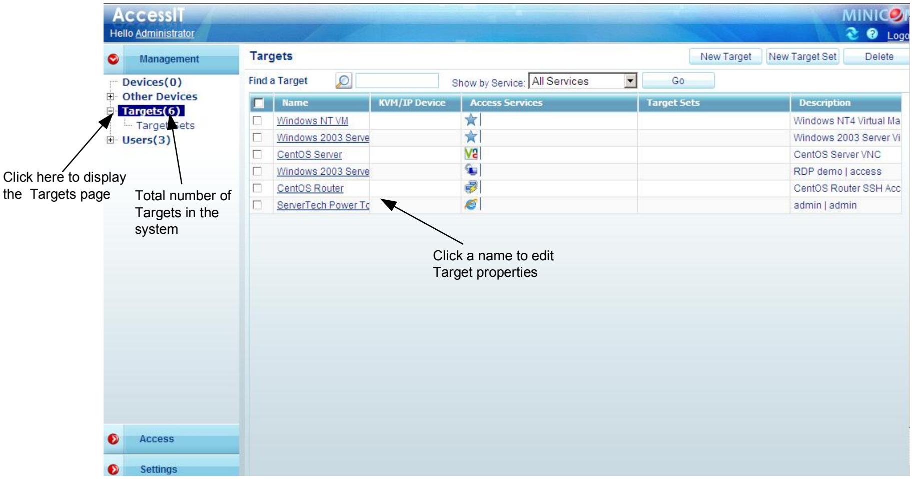
7. Configuring Targets

You must input the de tails of all the Targets physically connected to the system's IP devices / KVM switches. This includes giving each Target a unique name and other relevant details.

As mentioned in the pre-installation guidelines, Appendix A on page 134 contains 2 lists of all the details you need to prepare.

To configure a Target:

1. From the **Management** menu, select **Targets** the **Targets** page appears see Figure 22.



Find a Target

Show by Service: All Services

□	Name	KVM/IP Device	Access Services	Target Sets	Description
□	Windows NT VM		★		Windows NT4 Virtual Ma
□	Windows 2003 Serve		★		Windows 2003 Server Vi
□	CentOS Server				CentOS Server VNC
□	Windows 2003 Serve				RDP demo | access
□	CentOS Router				CentOS Router SSH Acc
□	ServerTech Power Tc				admin | admin

Figure 22 Target page

The columns display the following information:

- **Name** – Name of Target. You can search for a Target by typing the Target name in the **Find a Target** field. You can sort the names out in alphabetical order A-Z or Z-A by clicking the top of the **Name** column. You can also select which Targets to display from the **Show by Service** drop-down list. You can show all Targets or just show Targets with a particular Access Service, to do so choose the desired service from the **Show by Service** drop-down list.

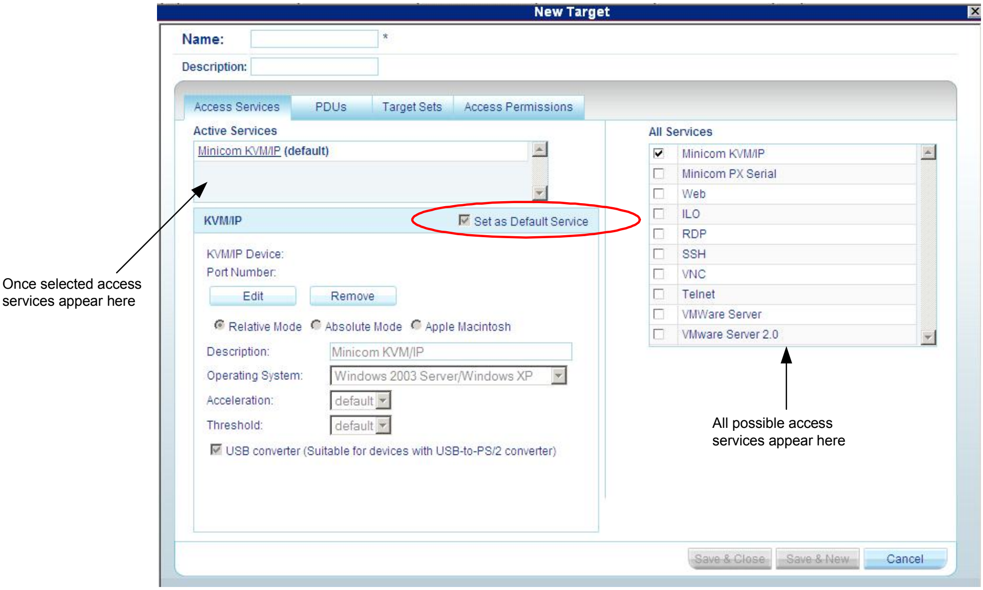
- **KVM/IP Device** – The name of the Minicom KVM/IP device, the target is connected to.

- **Access Services -** Icons of Access services available to access the target. To see which service the icon represents, hold the mouse over the icon and a tooltip appears with the name of the service.

- **Target Sets** – The Target Sets this Target is a member of.
- **Description** - optional description of the Target.

2. From the toolbar, click New Target. The **New Target** page appears, see Figure 23.

Name - Type a unique name for each server in the system.



New Target

Name: *

Description:

Access Services | PDUs | Target Sets | Access Permissions

Active Services

Minicom KVM/IP **(default)**

KVM/IP ☑ Set as Default Service

KVM/IP Device:

Port Number:

Edit | Remove

● Relative Mode ○ Absolute Mode ○ Apple Macintosh

Description: Minicom KVM/IP

Operating System: Windows 2003 Server/Windows XP

Acceleration: default

Threshold: default

☑ USB converter (Suitable for devices with USB-to-PS/2 converter)

All Services

☑ Minicom KVM/IP
□ Minicom PX Serial
□ Web
□ ILO
□ RDP
□ SSH
□ VNC
□ Telnet
□ VMWare Server
□ VMware Server 2.0

Save & Close | Save & New | Cancel

Once selected access services appear here

All possible access services appear here

Figure 23 New Target page

7.1 Access Services tab

Here you select and configure all access services relevant to this Target.

All Services / Active Services: – from the **All Services** list, select the checkbox of all access services relevant to this Target. Once selected the service appears in the **Active Services** list. Configured console servers also appear here (see section 9.2 on page 50).

Note! Below explains how to configure Minicom IP devices. Configuring other Access services is explained in section 11 on page 68.

The pre-installation guidelines on page 10 explained what information you need to configure each Target.

7.1.1 Default access service

You can set any of the access services to be the default service. This means that the service will be used to access the Target by default when selecting the Target by clicking the Target name. To access the Target via a different service, the service must be selected. To set a service as the default, display the service as explained below and select the **Set as Default Service** checkbox – circled in Figure 23.

7.1.2 Minicom KVM/IP

KVM/IP Device / Port number: Assign the IP device and KVM switch port number (where relevant) to which this Target is physically connected.

To do so:

1. Click Edit. The **Assign Device** window appears, see Figure 24.

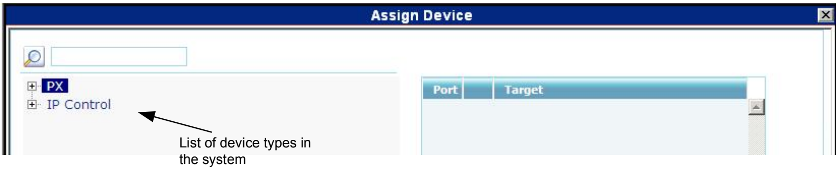
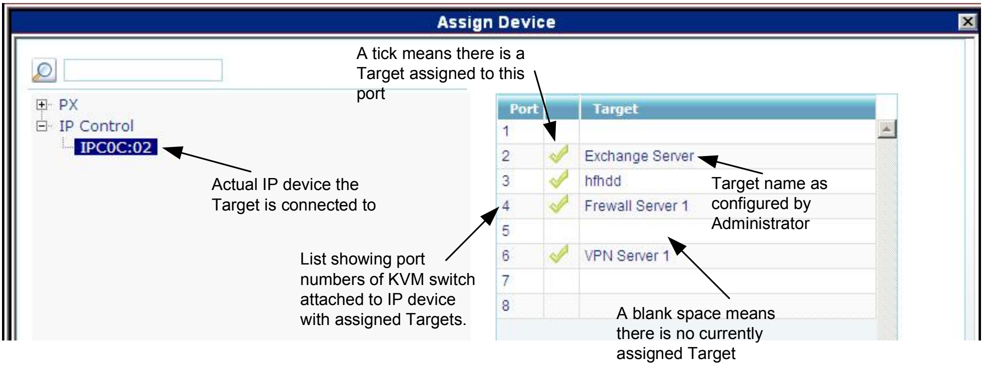


Figure 24 Assign Device window

2. From the list, expand the device type the target is connected to and select the actual device the target is connected to, see Figure 25.

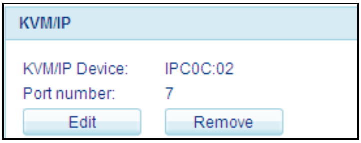

Assign Device
PX
IP Control
IPC0C:02
A tick means there is a Target assigned to this port
Actual IP device the Target is connected to
Target name as configured by Administrator
List showing port numbers of KVM switch attached to IP device with assigned Targets.
A blank space means there is no currently assigned Target

Port		Target
1		
2	✓	Exchange Server
3	✓	hfhdd
4	✓	Frewall Server 1
5		
6	✓	VPN Server 1
7		
8		

Figure 25 Device and Targets

3. Double-click the port number row to which the Target is connected. The name of the target appears in that row.

4. Click **Save**. The changes are saved and the **New Target** page reappears showing the assigned IP device and port number, see Figure 26.



KVM/IP

KVM/IP Device: IPC0C:02

Port number: 7

Figure 26 KVM/IP Device / Port number

To remove an assigned Target from an IP device/ KVM switch port click Remove. The assignment is removed.

Other KVM/IP elements are as follows:

Relative/Absolute mode/Apple Macintosh –

Absolute Mouse mode and Apple Macintosh are only relevant for PX USB KVM/IP devices. All other KVM/IP devices must have Relative Mouse Mode selected (which is the default).

For PX USB KVM/IP devices:

- If the Operating system on the Target is, Windows ME or later, Select Absolute Mouse mode.
- If the Operating system on the Target is, Windows 98 or Linux, Novell, UNIX or SUN, select Relative Mode.
- If the Target is a MAC computer, select Apple Macintosh.

Description – Type a description for the Target. E.g. Backup server.

Operating System – Select the operating system of the Target from the Drop-down list. The mouse parameter options adjust to match the operating system.

Acceleration / Threshold – When the Target's mouse settings are not default select the appropriate values. Match the values to that of the server's mouse.

Note! (Relevant to all IP devices except PX USB) For Windows XP and later. Go to the Mouse settings on the Target and uncheck Enhance pointer precision.

USB Converter - When an IP device connects to a server via a USB to PS/2 adapter, or ROC/RICC USB, or X RICC USB or Specter USB, select the **USB Converter** checkbox. The USB conversion affects the mouse emulation and the **USB Converter** helps to synchronize the mouse.

Also when an IP device is connected to a Linux server, select the "USB Converter" checkbox.

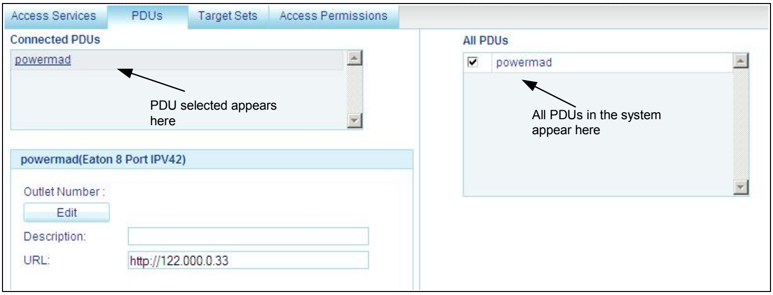
See section 11 on page 68 to configure other Access services.

7.2 PDUs tab

Where a Target is connected to a PDU, you must associate the PDU with the Target.

To do so:

1. Press the **PDUs** tab. The following appears.



Access Services | PDUs | Target Sets | Access Permissions

Connected PDUs

powermad

PDU selected appears here

powermad(Eaton 8 Port IPV42)

Outlet Number :

Edit

Description:

URL: http://122.000.0.33

All PDUs

☑ powermad

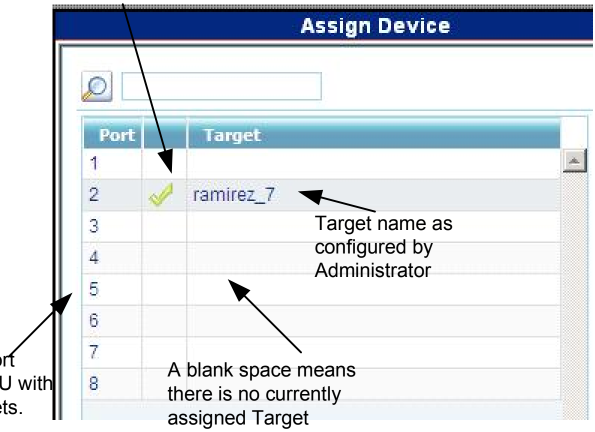
All PDUs in the system appear here

Figure 27 PDUs tab

2. Names of all configured PDUs appear in the **All PDUs** list. To configure a PDU see section 9 on page 48. From the **All PDUs** list, select the checkbox of the PDU the Target is connected to. The PDU appears in the **Connected PDUs** list with its details below this. Description and URL are input by an Administrator - explained in Section 9.

3. Click Edit to assign the outlet number to which this Target is physically connected. The **Assign Device** window appears, see Figure 28.

A tick means there is an assigned Target to this port



Assign Device

Port		Target
1		
2	✓	ramirez_7
3		
4		
5		
6		
7		
8		

Target name as configured by Administrator

List showing port numbers of PDU with assigned Targets.

A blank space means there is no currently assigned Target

Figure 28 Assign Device window

Tip! Instead of assigning an individual Target to a PDU outlet, you can assign all the PDU outlets to all relevant Targets as explained in section 9.1.1 on page 49.

4. Double-click the port number row to which the Target is connected. The name of the target appears in that row.

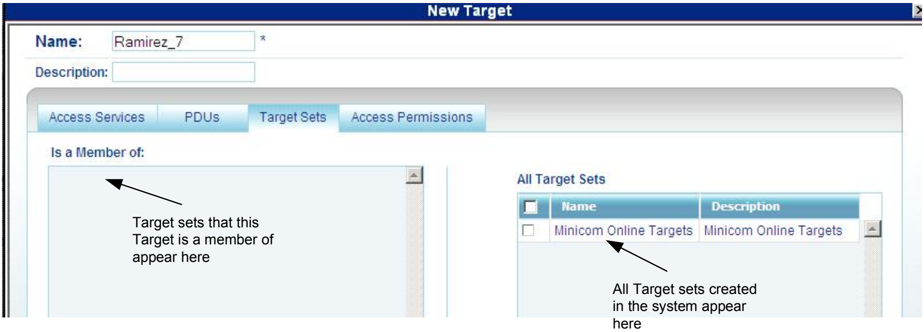
Note! You can assign the target to as many PDU ports or different PDUs as needed.

5. Click **Save**. The changes are saved and the **New Target** page reappears showing the assigned port number.

7.3 Target Sets tab

Creating Target Sets is explained in section 7.7 on page 36. Once you have created Target Sets you can put Targets into Target Sets, giving access rights to all Targets in a Set to all members.

1. Press the **Target Sets** tab. The following appears.



Name: Ramirez_7 *

Description:

Is a Member of:

All Target Sets

□	Name	Description
□	Minicom Online Targets	Minicom Online Targets

Target sets that this Target is a member of appear here

All Target sets created in the system appear here

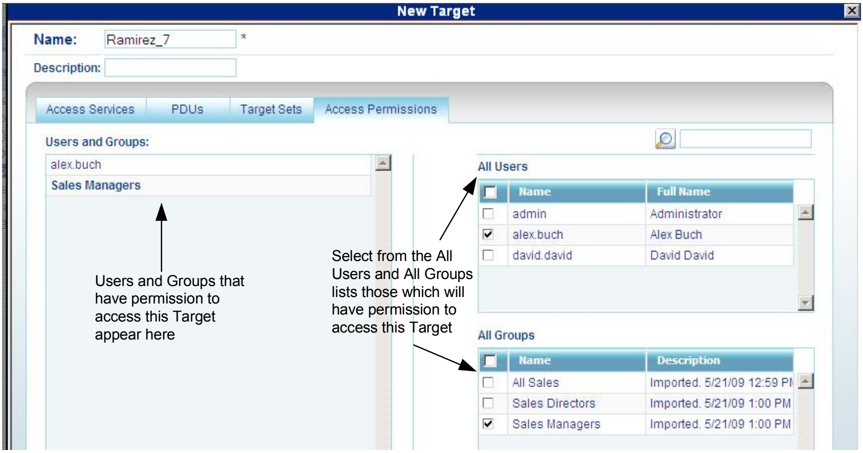
Figure 29 Target Sets

2. From the **All Target Sets** list, select the checkboxes of the Target Sets you want the Target to be associated with. The Target Set appears in the **Is a Member of** list.

7.4 Access Permissions tab

You can choose which Users and Groups can have access permission to the Target.

Press the **Access Permissions** tab. The following appears.



Name: Ramirez_7 *

Description:

Users and Groups:

alex.buch

Sales Managers

Users and Groups that have permission to access this Target appear here

Select from the All Users and All Groups lists those which will have permission to access this Target

All Users

□	Name	Full Name
□	admin	Administrator
☑	alex.buch	Alex Buch
□	david.david	David David

All Groups

□	Name	Description
□	All Sales	Imported. 5/21/09 12:59 PM
□	Sales Directors	Imported. 5/21/09 1:00 PM
☑	Sales Managers	Imported. 5/21/09 1:00 PM

Figure 30 Access Permissions tab

All existing Users appear in the **All Users** list. All Groups appear in the **All Groups** list.

To choose which Users / Groups have access to the Target:

1. Select the checkboxes of the Users or Groups. They appear in the **Users and Groups:** list.

To disassociate a User/Group from a Target:

Unselect the User/Group checkbox from the relevant list.

7.5 Saving the Target

Click Save & New. The Target details are now in the system.

Repeat this process to input all connected servers. When finished, click Save & Close. All Targets appear on the Targets page, see Figure 22.

(To edit a Target name or description click a Target on the Targets page).

7.6 Deleting Targets

You can remove Targets from the system as follows:

From the **Targets** page select the checkboxes of the Targets to be deleted.

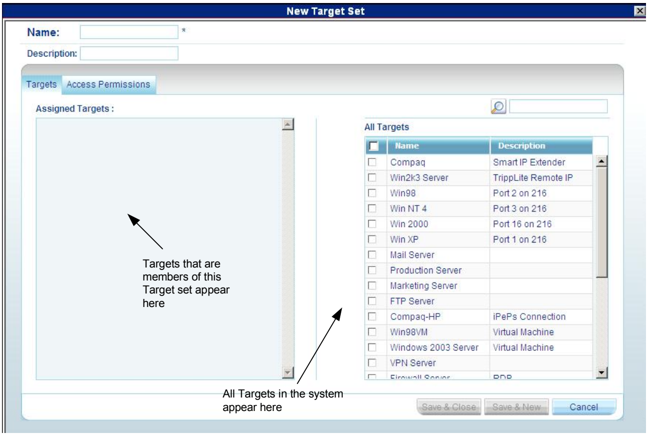
Press Delete. Press □ to select or deselect all checkboxes with one click.

7.7 Creating a Target Set

You can group Targets into sets. E.g. make a set of all financial servers in the system. You can then give users access rights per the Target Set rather than per individual Targets. Target Sets appear as a Favorites folder for users on the **Access** page.

To create a new Target Set:

1. From the **Targets** page, click New Target Set. The following appears.



☐	Name	Description
☐	Compaq	Smart IP Extender
☐	Win2k3 Server	TrippLite Remote IP
☐	Win98	Port 2 on 216
☐	Win NT 4	Port 3 on 216
☐	Win 2000	Port 16 on 216
☐	Win XP	Port 1 on 216
☐	Mail Server	
☐	Production Server	
☐	Marketing Server	
☐	FTP Server	
☐	Compaq-HP	iPePs Connection
☐	Win98VM	Virtual Machine
☐	Windows 2003 Server	Virtual Machine
☐	VPN Server	
☐	Firewall Server	RDP

Targets that are members of this Target set appear here

All Targets in the system appear here

Figure 31 New Target Set – Targets tab

2. **Name:** - Type a unique name for the Target set.

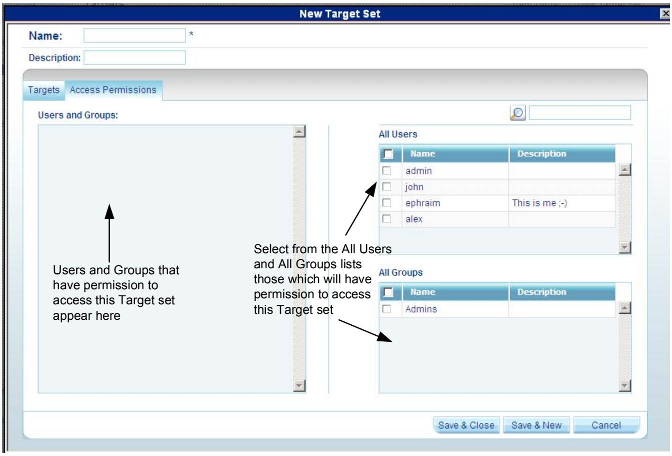
3. **Description** – Type a description.

4. From the **All Targets** list, select the checkboxes of the Targets you want to add to the Target set. The Targets appear in the **Assigned Targets** list.

7.7.1 Access Permissions tab

You can choose which Users and Groups can have access permissions to the Target set.

Press the **Access Permissions** tab. The following appears.



□	Name	Description
□	admin	
□	john	
□	ephraim	This is me ;-)
□	alex	

□	Name	Description
□	Admins	

Users and Groups that have permission to access this Target set appear here

Select from the All Users and All Groups lists those which will have permission to access this Target set

Figure 32 Access Permissions tab

All existing Users appear in the **All Users** list. All Groups appear in the **All Groups** list.

To choose which Users / Groups have access to the Target set:

1. Select the checkboxes of the Users or Groups. They appear in the **Users and Groups**: list.

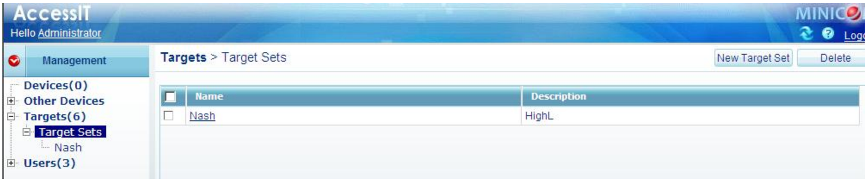
To disassociate a User/Group from a Target set:

Unselect the User/Group checkbox from the relevant list.

7.7.2 Saving the Target set

Click Save & New. The Target set details are now in the system.

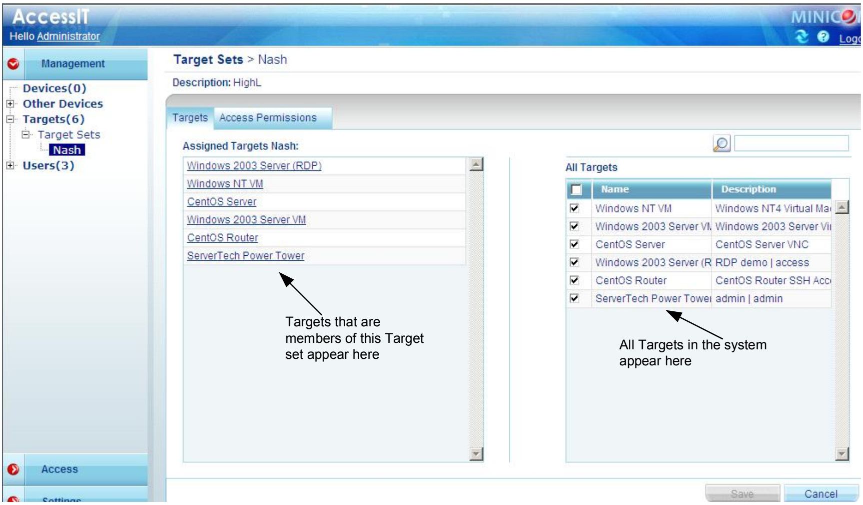
Repeat this process to add more Target sets. When finished, click Save & Close. All Target sets appear in the menu under **Targets/Target Sets** and also on the Target sets page, from the menu select Targets/Target Sets, see Figure 33.



□	Name	Description
□	Nash	HighL

Figure 33 Target sets page

To see all the Targets in a Target set, click the Target set name either from the menu, or on the page, see Figure 34. From this page you can at any time assign or remove Targets from the Target set, and from the **Access Permissions** tab choose which Users and Groups can have access permissions to the Target set, as explained on page 36. You can access Target properties by clicking a Target name in the **Assigned Targets** list.



Description: HighL

Assigned Targets Nash:

- Windows 2003 Server (RDP)
- Windows NT VM
- CentOS Server
- Windows 2003 Server VM
- CentOS Router
- ServerTech Power Tower

All Targets

☐	Name	Description
☑	Windows NT VM	Windows NT4 Virtual Ma
☑	Windows 2003 Server VI	Windows 2003 Server Vi
☑	CentOS Server	CentOS Server VNC
☑	Windows 2003 Server (R	RDP demo | access
☑	CentOS Router	CentOS Router SSH Acc
☑	ServerTech Power Towe	admin | admin

Targets that are members of this Target set appear here

All Targets in the system appear here

Figure 34 Target set

7.7.3 Deleting a Target Set

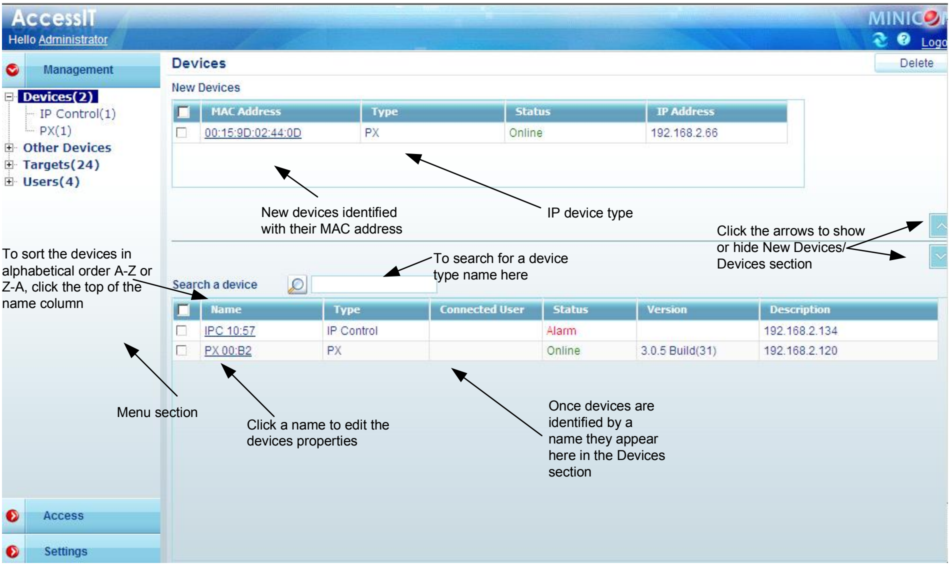
You can delete a Target set from the **Target Sets** page:

1. Select the checkboxes of the Target set to be deleted.
2. Press Delete. The Target set is removed. Press ☐ to select or deselect all checkboxes with one click.

Note: Deleting a Target set will not delete the individual Targets.

8. Configuring KVM/IP Devices

The web interface opens at the **Devices** page, see Figure 35. The **New Devices** section automatically displays all IP devices detected by the AccessIT system. (For IP devices to appear they must be configured to be Centralized Management enabled – see section 8.1 below). Each device appears identified by its MAC address. The MAC address of each IP device is written on a sticker on the unit's underside. Once the device is configured by giving it a name, it then only appears in the **Devices** section. The **New Devices** section itself only appears when there are new devices detected.



Devices

New Devices

☐	MAC Address	Type	Status	IP Address
☐	00:15:9D:02:44:0D	PX	Online	192.168.2.66

☐	Name	Type	Connected User	Status	Version	Description
☐	IPC 10:57	IP Control		Alarm		192.168.2.134
☐	PX 00:B2	PX		Online	3.0.5 Build(31)	192.168.2.120

New devices identified with their MAC address

IP device type

Click the arrows to show or hide New Devices/ Devices section

To sort the devices in alphabetical order A-Z or Z-A, click the top of the name column

To search for a device type name here

Menu section

Click a name to edit the devices properties

Once devices are identified by a name they appear here in the Devices section

Figure 35 Devices page

The columns on the **Devices** page display the following information:

Name – Once IP devices are given an identifying name they appear here.

Type – Connected IP device type.

Connected User – User currently operating the remote session.

Status

Under the Status column, there are the following possibilities:

> **Online –** The device is up and running and is ready to be configured or is available for a remote session.
>
> **Alarm –** Device is down and is unavailable for a remote session.

Warning – Problem with the device. See the **Devices** page on page 40 for more information.

Uploading – Device is receiving new firmware from AccessIT Manager.

Updating device – Device is receiving an updated configuration from AccessIT Manager.

Rebooting - Device reboots upon any Network parameter change, or firmware upgrade.

Connecting – AccessIT send or receives the Device Discovery message.

Version – Displays the device firmware version number.

Description – Identifying description of the device as input by the administrator when configuring the device.

8.1 Setting each IP device to be AccessIT enabled

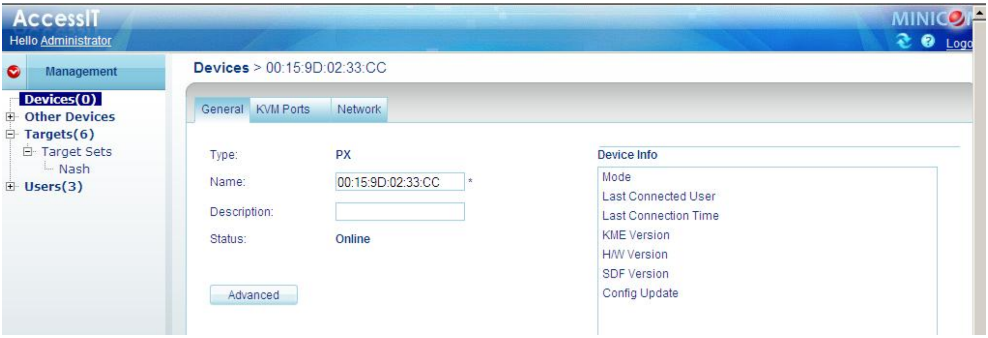
In order to be managed by AccessIT, all Minicom IP devices must be configured to be Centralized Management enabled. See section 4 on page 17.

Tip! Since IP devices only appear in the **New Devices** list once they are Centralized Management enabled, make each IP device Centralized Management enabled in a certain order with a suitable time gap, so that you can identify the unit’s location.

8.2 Configuring the IP devices

Configure a new IP device as follows:

1. In the **New Devices** section click the MAC address of an IP device. The **General** tab of the **Devices** page appears, see Figure 36.



Type: PX

Name: 00:15:9D:02:33:CC *

Description:

Status: Online

Figure 36 Devices page - General tab

Type – IP device type, PX, IP Control etc. (Read-only field).

Name - You must assign a unique name to each IP device before associating connected Targets or KVM switches. Type a name for the device.

Description – These are optional fields used for device identification.

Status – This is the connection status.

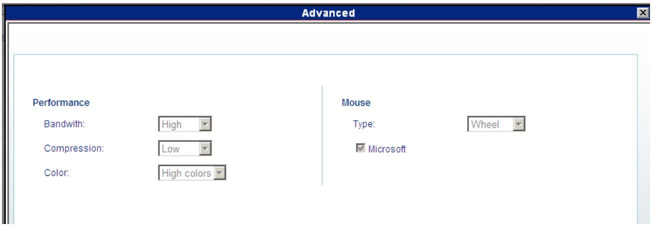
Device Info - contains information about the device, including its operational status and version numbers of firmware, KME (keyboard, mouse emulation), hardware, SDF (switch definition file) and date and time of last configuration update.

8.2.1 The Advanced button

When required, you can change the performance and mouse settings (the **Set mouse and performance from KVM/IP Session** must be unchecked on the Settings/Global Settings page - see section 13.1 on page 87).

To do so:

Press Advanced. The following appears:



Advanced

Performance

Bandwidth: High

Compression: Low

Color: High colors

Mouse

Type: Wheel

☑ Microsoft

Figure 37 Advanced page

8.2.2 Performance

Bandwidth has the following options from the drop-down menu:

High

For optimal performance while working with a Local Area (LAN) connection, select **High** bandwidth. This will adjust the performance to low compression and high color (16bit).

Low

For optimal performance when using a Dialup connection, select **Low** bandwidth. This will adjust the performance to high compression and 16 colors. For improved performance, verify that the **Color** selection is a 16 colors palette.

Medium

When working on DSL, cable or ISDN connections, select **Medium**.

Custom

Custom gives you the option to manually choose both the compression and colors.

8.2.3 Mouse

Select the appropriate values according to the type of mouse connected to the device.

Type - Select the mouse type you would like IP device to emulate. When setting the mouse emulation type, set it to match the mouse connected to the Local Console port on the IP device, e.g. if the local mouse is a 2 button mouse, but not from Microsoft set the Mouse Emulation type to **Standard Mouse** and uncheck the **Microsoft** checkbox.

Tip! The mouse on most KVM drawers in a standard rack is a **Standard Mouse**

Microsoft - Uncheck this box if the mouse does not work using Microsoft mouse protocol.

Important!!

We recommend not changing the Advanced settings unless there is erratic mouse behavior. E.g. the mouse makes random clicks and jumps arbitrarily around the screen.

Press **Apply** to save changes and return to the Device Properties page.

8.3 KVM Ports tab

In the **KVM Ports** tab you:

- Associate the KVM switches in the system to the relevant IP device
- Associate Targets with the relevant IP device/port number on the KVM switch

Click the **KVM Ports** tab, the following appears.

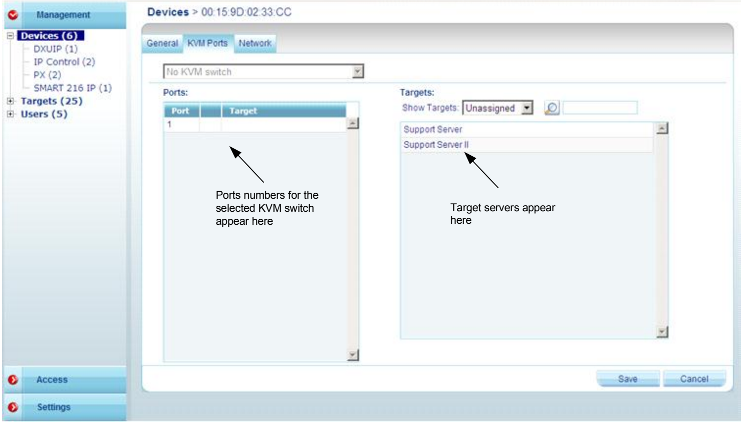


Figure 38 KVM Ports tab

The KVM switch drop-down list consists of pre-selected KVM switches. You must select all the KVM switch types physically connected to the system, this is done in the **Settings** part of the menu and is explained in section 14.2 on page 90. Select the KVM switch model (if any) physically connected to this IP device. The number of ports in the selected KVM switch appears in the **Ports** section.

Notes:

When using a Smart 116 IP, “**IP 116**” is selected by default and cannot be altered.

When using a Smart 216 IP or Smart 232 IP, “**Internal**” is selected by default and cannot be altered.

8.3.1 DXU IP II units

When there are DXU IP II units in the system:

For Centralized Management **enabled** select the correct DX configuration with **Ctrl** (and not PRT-SCR hotkey), as selected in the **KVM Switches** page.

For **managed** mode select the correct DX configuration with **PRT-SCR** (and not Ctrl hotkey), as selected in the **KVM Switches** page. Once the correct DX configuration with **PRT-SCR** is selected, the fields circled in Figure 39 appear.

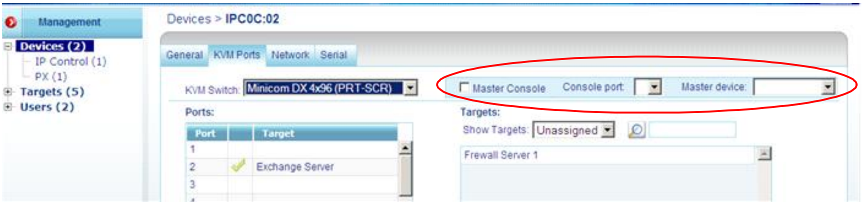


Figure 39 DXUIP II fields in AccessIT Managed mode

If this DX User IP II is the IP device connected to User port 1 of the DX Central, select the **Master Console** checkbox. (This enables the DX port statuses to be displayed in the AccessIT interface). If this unit is not the Master console, select the User port this device is connected to from the **Console port** drop-down list and select the Master device from the **Master device** drop down list.

Note! When there are more than one DXU IP II units in the system you must select the KVM switch file for all DXU IP II units.

8.4 Targets

The Targets you created appear in the **Targets** list.

You can choose to display all Targets or just unassigned Targets (default) or Targets belonging to a Target set. Select the desired option from the **Show Targets** drop-down menu.

You must associate the Targets with the relevant IP device or with the port numbers on the KVM switch to which they are physically connected.

To associate the Targets:

1. From the **Targets** list, double-click the Target connected port #1 of the KVM switch. The Target assigns to the port #1 of the Ports section. Alternatively drag and drop the Target to the correct port number.
2. Repeat the above step for all Targets connected. Ensure the right Target assigns to the correctly numbered port.

To remove a Target from a port:

Double-click the Target in the **Ports** section. The Target name moves to the **Target** section and is now unassigned.

Note! Deleting a Target removes its association with the KVM port number. See page 35.

When there is more than one DXU IP II units or if there are multi-user matrix KVM switches in the system, you must assign the same Targets to the same ports for each DXU IP II unit/matrix KVM switch.

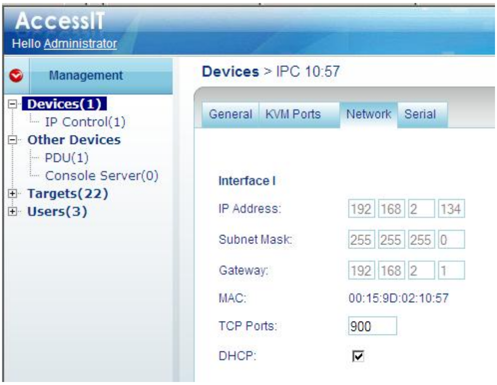
1. Assign the ports for one DXU IP II unit/matrix KVM switch.
2. Go to the **Devices** page and select the next DXU IP II unit/matrix KVM switch.
3. Click the **Targets** tab and in the **Show Targets** drop-down menu select **All Targets**.
4. Go down the list and again assign the same Targets to the same ports for this DXU IP II unit/matrix KVM switch.

When selecting a Target the AccessIT checks which DXU IP II unit/IP device connected to a matrix KVM switch, is available and automatically connects you to the chosen Target. If a local DX User is accessing the port View Only is available.

8.5 Network tab

In the Network tab you configure and modify Network parameters of the IP device.

Click the **Network** tab. The following appears.



Interface I

IP Address: 192 168 2 134

Subnet Mask: 255 255 255 0

Gateway: 192 168 2 1

MAC: 00:15:9D:02:10:57

TCP Ports: 900

DHCP: ☑

Figure 40 Network tab

Interface I displays the IP address of the IP device as discovered by the AccessIT Manager system. You can change this address here.

Enter **IP address, Subnet Mask** and **Default Gateway** for the network adapter, as given by your Network Administrator.

In **TCP Port** type a port number (from 800 and up to 65535). By default the port number is 900. This default port is suitable for the majority of installations.

Click to clear or select the following according to your requirements:

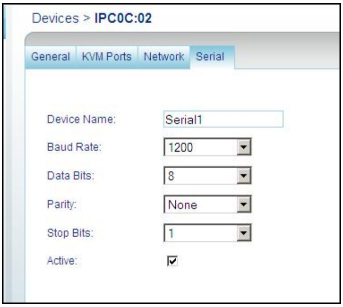
DHCP – Enable DHCP to provide you with dynamic IP addressing for the IP device, if a DHCP server exist.

Note: Any change in the Network configuration forces the IP device to restart.

8.5.1 Serial tab

In the **Serial** tab you define the console parameters for controlling RS232 Serial devices for KVM/IP units.

Click the **Serial** tab. The following appears.



Device Name: Serial1

Baud Rate: 1200

Data Bits: 8

Parity: None

Stop Bits: 1

Active: ☑

Figure 41 Serial tab

You can access a Serial device during a remote session by emulating its Serial connection via RS232 (VT100 & TTY).

Device Name - Type the name of the device (i.e. PowerManagement; Ciscorouter; - no spaces allowed in the device name).

Baud Rate, Data Bits, Parity, Stop bits - type the appropriate values according to the RS232 device line settings, attached to the KVM/IP device.

Active – Select **Active** to display the device on the Client toolbar.

8.6 Saving the IP device configuration changes

Press **Save** to save the settings and configure the IP device. The IP device is upgraded to the device firmware stored in the AccessIT system. It receives the SDF (Switch Definition File) from the AccessIT system and also a list of Targets, Users and their permissions (CFG). The IP device may be unavailable during the upgrade and while receiving the CFG and SDF updates.

8.7 Deleting IP devices

IP devices can be deleted from the AccessIT system from the **Devices** page.

To delete IP devices:

1. From the **Management** menu, click **Devices** the **Devices** page appears.
2. Select the checkboxes of the units to be deleted, or select the top checkbox to select or deselect all checkboxes.
3. Click Delete. The devices are deleted.

4. Uncheck **Enable** Centralized Management on the device's **Network Configuration** Web page. This will prevent the deleted IP device from being rediscovered.

8.8 Device discovery

The status of the IP devices is updated automatically every minute. You can manually discover new devices at any time.

To do so:

In the menu, right-click **Devices**, the **Discovery** menu appears, see Figure 42.

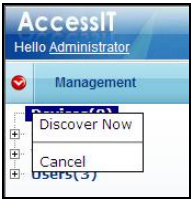


Figure 42 Discovery menu

Click **Discover Now**. The AccessIT Manager performs a device discovery on the network segment. All newly discovered devices appear in the **New Devices** section. All configured devices are rediscovered and a device configuration file (CFG) is sent to the devices. This process may take some time, during which the devices may be unavailable.

9. Configuring Other Devices

You must configure all the Power Distribution Units (PDU) and Console servers physically connected to the system's Targets.

From the menu, click **Other Devices**, the following appears.

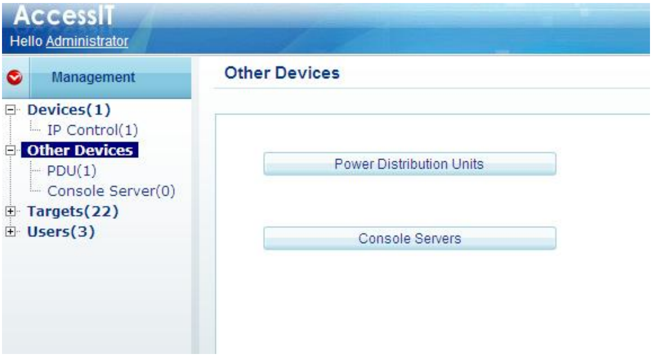


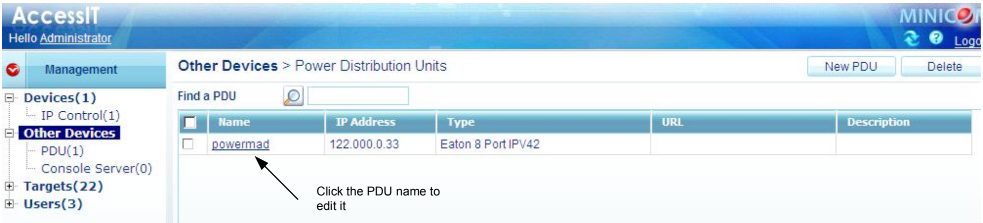
Figure 43 Other Devices

9.1 Configuring PDUs

Before configuring a PDU, you must define all the PDU types physically connected to the system, this is done in the Settings part of the menu and is explained in section 14.1 on page 89.

To configure a PDU:

1. Click Power Distribution Units or **PDU** from the menu. The Power Distribution Units page appears.



□	Name	IP Address	Type	URL	Description
□	powermad	122.000.0.33	Eaton 8 Port IPV42		

Click the PDU name to edit it

Figure 44 Power Distribution Units page

The columns display the following information:

- **Name** – Name of PDU. You can search for a PDU by typing the PDU name in the **Find a PDU** field. You can sort the names out in alphabetical order A-Z or Z-A by clicking the top of the **Name** column.
- **IP address** – The IP address of the PDU

- **Type** – Type of PDU (as selected in the Settings section, see page 89)
- **URL** / **Description** - The PDU’s URL for its web based management access and optional description of the PDU

2. From the toolbar, click New PDU. The **New PDU** page appears, see Figure 23.

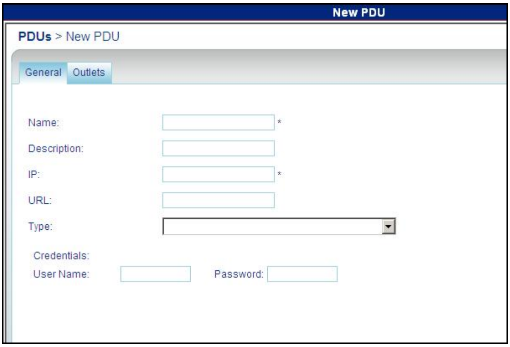


Figure 45 PDU – General tab

Name - Type a unique name for the PDU.

Description - Type an optional description of the PDU.

IP address – Type the IP address of the PDU.

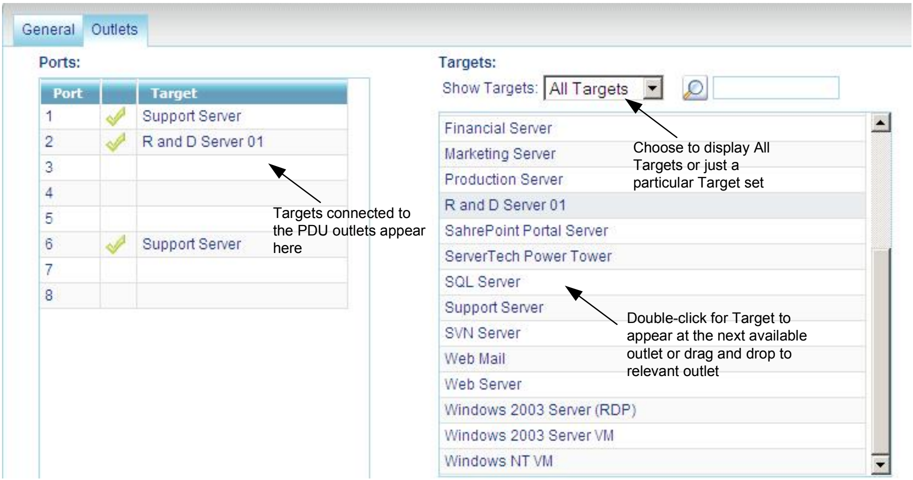
URL –Type the URL of the PDU. (Generally the URL is the same as the IP address)

Type – Select the PDU type from the drop-down list. The PDU drop-down list consists of pre-defined PDUs.

Credentials – Type the username and password to access the PDU

9.1.1 Outlets tab

Click the Outlets tab, Figure 50 appears. The Ports list shows the number of ports of the PDU type selected.



Ports:

Port		Target
1	✓	Support Server
2	✓	R and D Server 01
3		
4		
5		
6	✓	Support Server
7		
8		

Targets connected to the PDU outlets appear here

Targets:

Show Targets: All Targets

Choose to display All Targets or just a particular Target set

- Financial Server
- Marketing Server
- Production Server
- R and D Server 01
- SahrePoint Portal Server
- ServerTech Power Tower
- SQL Server
- Support Server
- SVN Server
- Web Mail
- Web Server
- Windows 2003 Server (RDP)
- Windows 2003 Server VM
- Windows NT VM

Double-click for Target to appear at the next available outlet or drag and drop to relevant outlet

Figure 46 Outlets tab

Here you select and configure all Targets connected to the PDU ports.

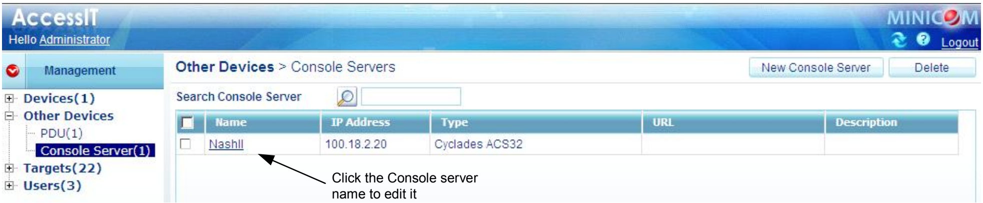
1. From the Show Targets drop-down list choose to display all Targets or only the particular Target set that has servers connected to the PDU. The Targets appear in the list. You can search for a Target set by typing the Target set name in the field.
2. Double-click a Target from the Targets list to make it appear in the first available spot in the Ports list. For example if Target1 is connected to to port 1 of the PDU, double-click Target1, etc. Drag and drop a Target to place it into any port number of the Ports list. E.g. if Target1 is connected to to port 7 of the PDU, drag and drop Target1 to port 7.
3. On completeion click Save. The PDU appears on the PDU page, see Figure 44. Also when clicking a Target on the Targets page, the configured PDU appears in the PDU tab, see Figure 27. Power management is operated through the PDU icon that appears next to the Target on the Access page, see page 108.

9.2 Configuring Console Servers

Before configuring a Console server you must select all the Console Server types physically connected to the system, this is done in the **Settings** part of the menu and is explained in section 14.3 on page 92.

To configure a Console server:

1. Click Console Servers or **Console Servers** from the menu. The Console Servers page appears.



Other Devices > Console Servers

Search Console Server

□	Name	IP Address	Type	URL	Description
□	Nashll	100.18.2.20	Cyclades ACS32		

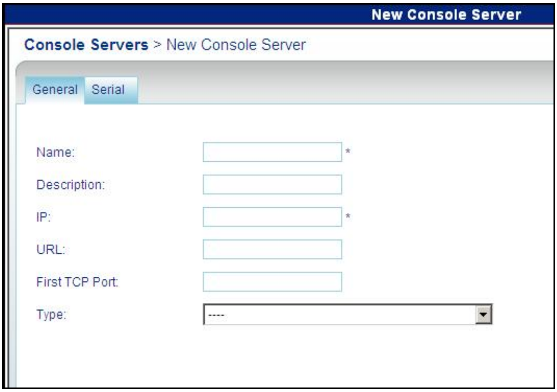
Click the Console server name to edit it

Figure 47 Console Servers page

The columns display the following information:

- **Name** – Name of Console Server. You can search for a Console Server by typing the name in the **Search Console Server** field. You can sort the names out in alphabetical order A-Z or Z-A by clicking the top of the **Name** column.
- **IP address** – The IP address of the Console Server
- **Type** – Type of Console Server
- **URL** / **Description** - The URL of the Console Server's web management interface and optional description of the Console Server

2. From the toolbar, click New Console Server. The **New Console Server** page appears, see Figure 48.



Console Servers > New Console Server

Name: *

Description:

IP: *

URL:

First TCP Port:

Type: ----

Figure 48 Console Server – General tab

Name - Type a unique name for the Console Server.

Description - Type an optional description of the Console Server.

IP – Type the IP address of the Console Server.

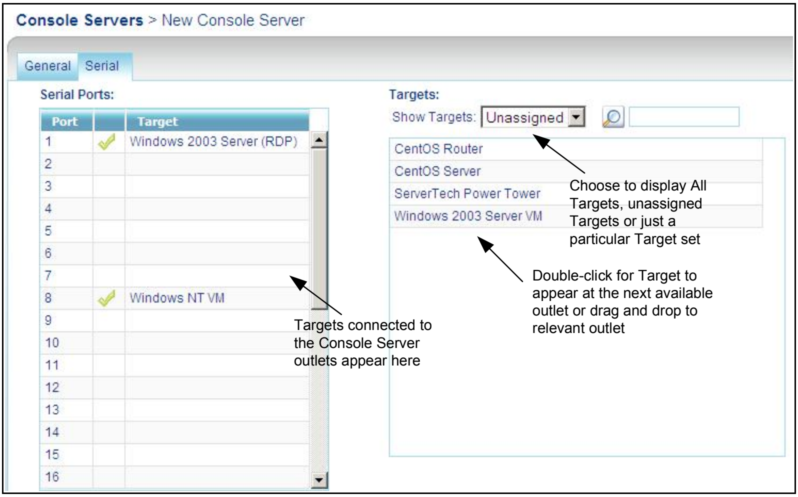
URL – Type the URL of the Console Server's web management interface (generally it's the same as the IP address).

First TCP Port – Type the first TCP Port of the Console Server.

Type – Select the Console Server type from the drop-down list. The Console Server drop-down list consists of pre-selected Console Servers. (Explained in section 14.3 on page 92).

9.2.1 Serial tab

Click the Serial tab, Figure 49 appears. The Ports list shows the number of ports of the Console Server type selected.



Console Servers > New Console Server

Serial Ports:

Port		Target
1	✓	Windows 2003 Server (RDP)
2		
3		
4		
5		
6		
7		
8	✓	Windows NT VM
9		
10		
11		
12		
13		
14		
15		
16		

Targets:

Show Targets: Unassigned

- CentOS Router
- CentOS Server
- ServerTech Power Tower
- Windows 2003 Server VM

Choose to display All Targets, unassigned Targets or just a particular Target set

Double-click for Target to appear at the next available outlet or drag and drop to relevant outlet

Targets connected to the Console Server outlets appear here

Figure 49 Serial tab

Here you select and configure all Targets connected to the Console Server ports.

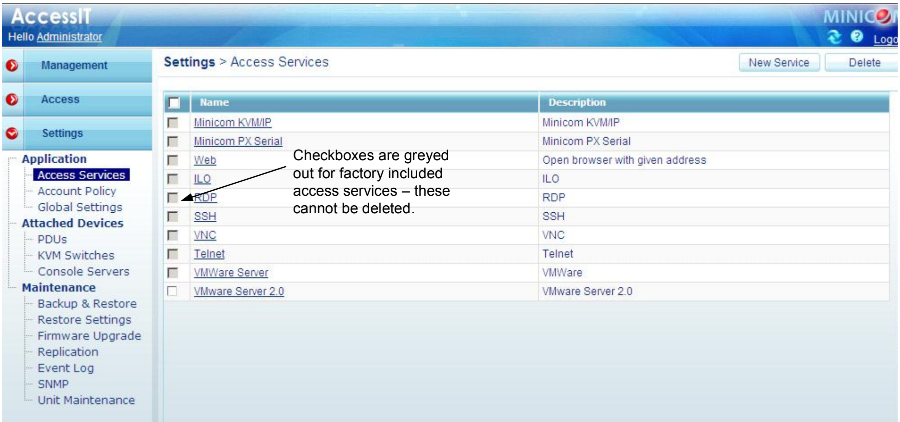
1. From the Show Targets drop-down list choose to display all Targets or only the particular Target set that has servers connected to the Console Server. The Targets appear in the list. You can search for a Target set by typing the Target set name in the field.

2. Double-click a Target from the Targets list to make it appear in the first available spot in the Ports list. For example if Target1 is connected to to port 1 of the Console Server, double-click Target1, etc. Drag and drop a Target to place it into any port number of the Ports list. E.g. if Target1 is connected to to port 7 of the Console Server, drag and drop Target1 to port 7.

3. On completeion click Save. The Console Server appears on the Console Server page, see Figure 47. It also appears as an icon on the Access page in the More Access Services column - see page 108, and also as a service in the New Target page, see page 30.

10. Configuring Access Services

From the menu, click **Settings**. The **Access Services** page appears see Figure 50.



☐	Name	Description
☐	Minicom KVM/IP	Minicom KVM/IP
☐	Minicom PX Serial	Minicom PX Serial
☐	Web	Open browser with given address
☐	ILO	ILO
☐	RDP	RDP
☐	SSH	SSH
☐	VNC	VNC
☐	Telnet	Telnet
☐	VMWare Server	VMWare
☐	VMware Server 2.0	VMware Server 2.0

Checkboxes are greyed out for factory included access services – these cannot be deleted.

Figure 50 Access Services

10.1 Access services

Besides connecting to Minicom KVM/IP devices, you can connect to a variety of both hardware and software external resources from the AccessIT interface as follows:

- Minicom PX Serial
- Web service
- ILO - HP Integrated Lights-Out (iLO 2 only)
- RDP - Remote Desktop Protocol
- SSH - Secure Shell
- VNC- Virtual Network Computing
- Telnet- TELecommunication NETwork
- VMware Server (VMware Server 1.x only)

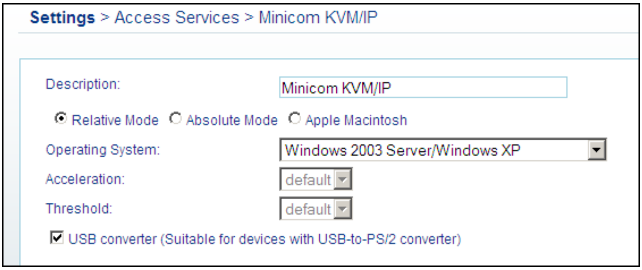
See page 15 - 16 for an elaboration of the above services.

From the **Access Services** page you can configure access services for Targets in the system. You can also add new Access services from this page.

Outlined below, is the default template values for all the Access Services. If these values are not suitable you can change them.

10.2 Minicom KVM/IP

Click **Minicom KVM/IP**. The Minicom KVM/IP settings appear, see Figure 51.



Settings > Access Services > Minicom KVM/IP

Description: Minicom KVM/IP

● Relative Mode ○ Absolute Mode ○ Apple Macintosh

Operating System: Windows 2003 Server/Windows XP

Acceleration: default

Threshold: default

☑ USB converter (Suitable for devices with USB-to-PS/2 converter)

Figure 51 Minicom KVM/IP settings

The default elements of the Minicom KVM/IP settings as follows:

Note! Only change the default settings if the large majority of the Targets in the system have settings that are different to the default settings.

Description – This is the description of the Access service - Minicom KVM/IP device.

Relative/Absolute mode/Apple Macintosh –

Absolute Mouse mode and Apple Macintosh are only relevant for PX USB KVM/IP devices. All other KVM/IP devices must have Relative Mouse Mode selected (which is the default).

For PX USB KVM/IP devices:

- If the Operating system on the Target is, Windows ME or later, select Absolute Mouse mode.
- If the Operating system on the Target is, Windows 98 or Linux, Novell, UNIX or SUN, select Relative Mode.
- If the Target is a MAC computer, select Apple Macintosh.

Operating System – Default operating system is Windows 2003 Server/Windows XP. This setting is suitable for Windows XP and later. If the large majority of the Targets in the system have a different operating system, select it from the Drop-down list. The mouse parameter options adjust to match the operating system.

Acceleration / Threshold – When the Target's mouse settings are not default select the appropriate values. Match the values to that of the server's mouse.

Note! (Relevant to all IP devices except PX USB) For Windows XP and later. Go to the Mouse settings on the Target and uncheck Enhance pointer precision.

USB Converter - When a KVM/IP device connects to a server via a USB to PS/2 adapter, or RICC/ROC USB, or X RICC USB or Specter USB, select the **USB Converter** checkbox. The USB conversion affects the mouse emulation and the **USB Converter** helps to synchronize the mouse.

10.3 Configuring other Access Services – introduction

The template values are automatically applied to new Targets that have the Access Service assigned to them.

For example, there is a default value for the application path of an access service. If this is suitable, ensure that all users have the access service application in the same path on their computer. Where a user computer has a different path, a prompt appears on the user's computer asking the user to browse for the Access Service application on his computer.

Note! Access Service settings can also be changed if necessary, for individual Targets, explained on page 68.

10.3.1 Access Services default values

Below are the factory included access services and their default values. If these values are not suitable you can change them. If an Access Service has an executable application, the application must be installed on all client computers.

10.3.2 General note about application paths

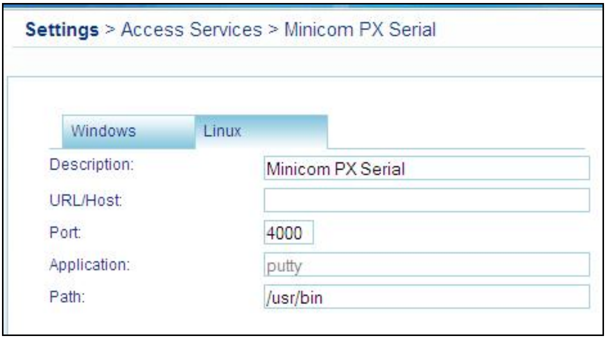
When inputting the application path into the AccessIT client interface you can include variables. For example for an access service called ABC service, by typing "%ProgramFiles%\ABCservice" the application could be installed in any drive on client computers in the Program Files\ABCservice folder.

The following variables in the application path can be used:

- %ProgramFiles% - Program Files folder
- %SystemRoot% - Windows folder

10.3.3 Minicom PX Serial

Click **Minicom PX Serial**. The Minicom PX Serial settings appear, see Figure 52



Settings > Access Services > Minicom PX Serial

Description: Minicom PX Serial

URL/Host:

Port: 4000

Application: putty

Path: /usr/bin

Figure 52 Minicom PX Serial settings

Windows/Linux tab – Select the operating system by clicking the appropriate tab. For each system the PuTTy Application Path is different.

Description: - Description of the access service - Minicom PX Serial.

Application: - PuTTy.exe is application used and it must be installed on all client computers, see the paragraph below.

The PuTTy application can be obtained from:
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

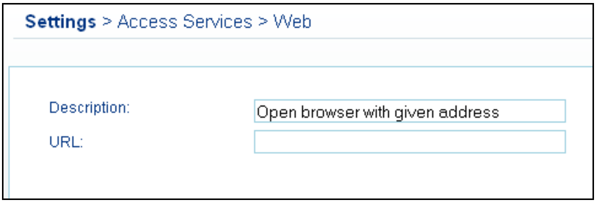
Path: - PuTTy application must be installed on all client computers, preferably in the same path. In the Windows default path %ProgramFiles%\PuTTy, see Figure 52, the application could be in any drive in the Program Files\PuTTy folder. See the General notes above about variables.

URL/Host: - Type the URL/Host of the Minicom PX Serial.

Port: - The Minicom PX Serial, TCP port number is 4000.

10.3.4 Web

Click **Web**. The Web settings appear, see Figure 53.



Settings > Access Services > Web

Description: Open browser with given address

URL:

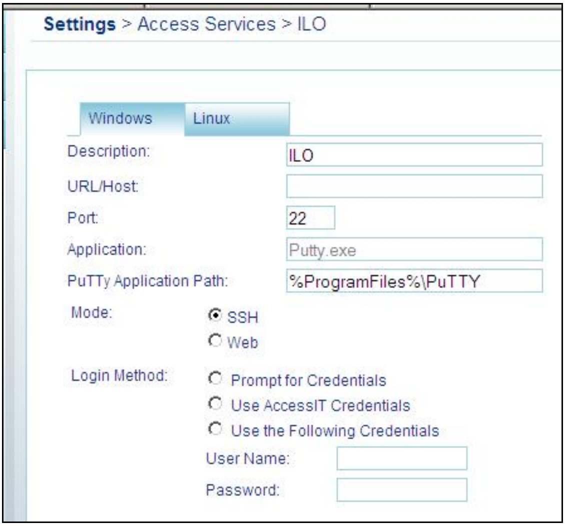
Figure 53 Web Target

Description: - Default description.

Set the URL for each individual web page as explained on page 69.

10.3.5 ILO

Click **ILO**. The ILO settings appear, see Figure 54. This supports iLO 2 only.



Settings > Access Services > ILO

Description: ILO

URL/Host:

Port: 22

Application: Putty.exe

PuTTy Application Path: %ProgramFiles%\PuTTY

Mode: ● SSH ○ Web

Login Method: ○ Prompt for Credentials ○ Use AccessIT Credentials ○ Use the Following Credentials

User Name:

Password:

Figure 54 ILO – SSH mode

Windows/Linux tab – Select the operating system by clicking the appropriate tab. For each system the PuTTy Application Path is different.

Description – Description of the access service - ILO.

URL/Host – Type the URL/Host of the ILO resource.

Port / Application / PuTTy Application Path – these fields are only relevant in SSH mode. The difference between SSH and Web mode is detailed below.

SSH mode (default)

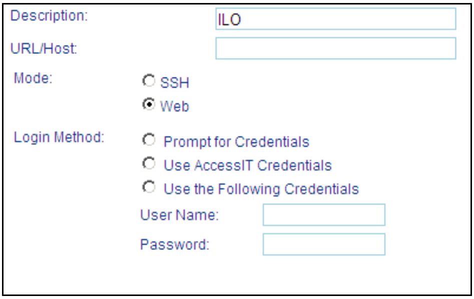
SSH mode uses an ILO console server. In SSH mode the PuTTy application must be installed on all client computers, preferably in the same path. In the Windows default path %ProgramFiles%\PuTTy - see Figure 54 – the application could be in any drive in the Program Files\PuTTy folder. See the General notes above about variables.

The PuTTy application can be obtained from: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

In SSH mode, the port number is 22 (default).

Web mode

Web mode uses a remote console with power management options. In Web mode there is no need for an executable application. Figure 55 illustrates the ILO fields in Web mode.



Description: ILO

URL/Host:

Mode: ○ SSH ● Web

Login Method: ○ Prompt for Credentials ○ Use AccessIT Credentials ○ Use the Following Credentials

User Name:

Password:

Figure 55 ILO – Web mode

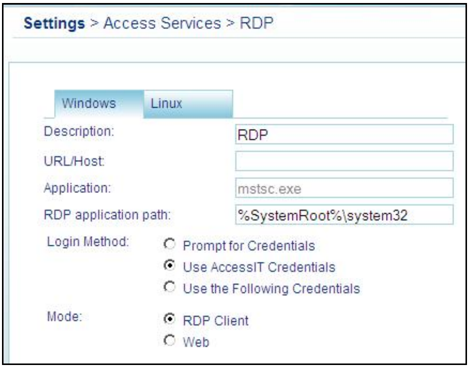
Login Method:

- Prompt for Credentials – this means the ILO 2 login page appears and you login manually.
- Use AccessIT Credentials – this means AccessIT logs into ILO 2 with the currently logged user credentials. Ensure that ILO 2 is configured to recognize the same username and password.
- Use the Following Credentials – Where the username and password are different for AccessIT and ILO 2, select this option. User Name and Password fields appear. Type the ILO 2 User Name and Password. AccessIT logs into ILO 2 using this User Name and password.

Note! ILO 2 web mode with automatic login is supported in Internet Explorer only. With Firefox the ILO 2 login page appears and users have to login manually.

10.3.6 RDP

Click **RDP**. The following are the default settings for RDP.



Settings > Access Services > RDP

Description: RDP

URL/Host:

Application: mstsc.exe

RDP application path: %SystemRoot%\system32

Login Method:
○ Prompt for Credentials
● Use AccessIT Credentials
○ Use the Following Credentials

Mode:
● RDP Client
○ Web

Figure 56 RDP– RDP Client mode

Windows/Linux tab – Select the operating system by clicking the appropriate tab. For each system the application path is different.

Description: - Description of the access service - RDP.

URL/Host: - Type the URL/Host of the RDP resource.

Mode: - RDP Client or Web. These are explained below.

RDP Client mode (default)

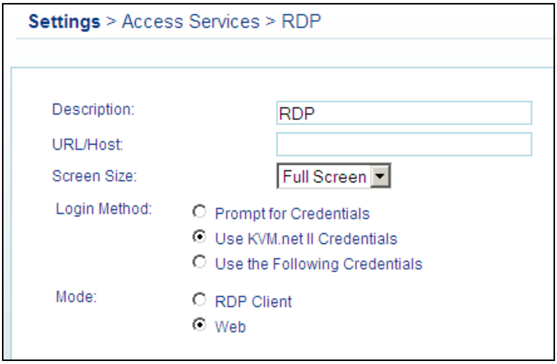
RDP Client mode uses an RDP console server. From Windows XP onwards the executable application - mstsc.exe - comes as part of the operating system. For Windows 2000 download the Client portion of the Remote desktop software from the Microsoft website.

Windows/Linux tab – Select the operating system by clicking the appropriate tab. For each system the default RDP Application Path is different.

RDP Application Path: - The RDP application must be installed on all local computers, preferably in the same path.

Web mode

When selecting Web mode, the page appears as in Figure 57.



Settings > Access Services > RDP

Description: RDP

URL/Host:

Screen Size: Full Screen

Login Method:
○ Prompt for Credentials
● Use KVM.net II Credentials
○ Use the Following Credentials

Mode:
○ RDP Client
● Web

Figure 57 RDP – Web mode

Web mode uses a remote console with power management options. In Web mode there is no need for an executable application.

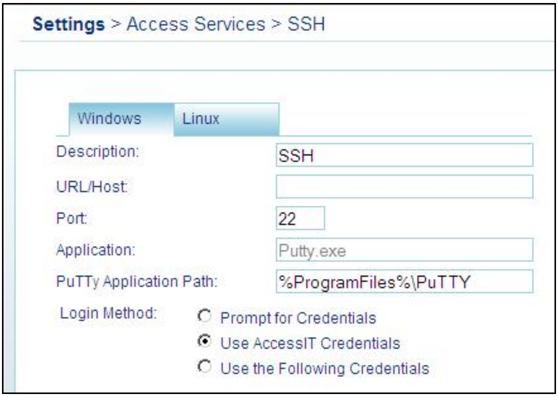
Screen Size: select the screen size from the drop-down menu.

Login Method: -

- Prompt for Credentials – this means the RDP login page appears and you login manually.
- Use AccessIT Credentials – this means AccessIT logs into RDP with the currently logged user credentials. Ensure that the Target computer is configured to recognize the same username and password.
- Use the Following Credentials – Where the username and password are different for AccessIT and the Target computer, select this option. User Name and Password fields appear. Type the RDP User Name and Password. AccessIT logs into the Target computer using this User Name and Password.

10.3.7 SSH

Click **SSH**. The following are the default settings for SSH.



Settings > Access Services > SSH

Description: SSH

URL/Host:

Port: 22

Application: Putty.exe

PuTTy Application Path: %ProgramFiles%\PuTTY

Login Method:
○ Prompt for Credentials
● Use AccessIT Credentials
○ Use the Following Credentials

Figure 58 SSH

Windows/Linux tab – Select the operating system by clicking the appropriate tab. For each system the default PuTTy Application Path is different.

Description: - Description of the access service - SSH.

Application - PuTTy.exe is the application used for SSH access. The PuTTy application can be obtained from:
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

PuTTy Application Path: - PuTTy application must be installed on all client computers, preferably in the same path. In the Windows default path %ProgramFiles%\PuTTy – see Figure 58 – the application could be in any drive in the Program Files\PuTTy folder. See the General notes above about variables.

URL/Host: - Type the URL/Host of the SSH resource.

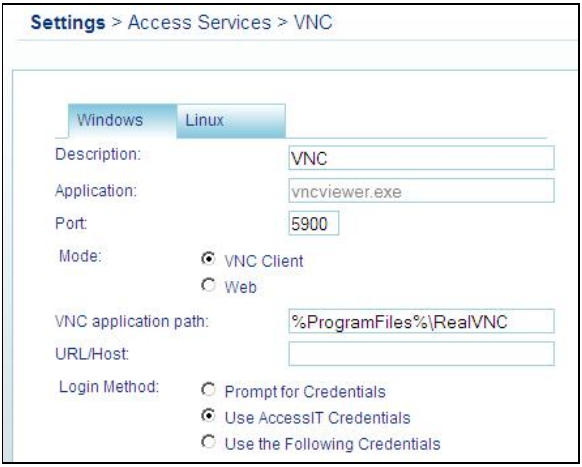
Port – The SSH port number is 22 (default).

Login Method

- Prompt for Credentials – this means the SSH login appears and you login manually.
- Use AccessIT Credentials – this means AccessIT logs into SSH with the currently logged user credentials. Ensure that SSH is configured to recognize the same User Name and Password.
- Use the Following Credentials – Where the username and password are different for AccessIT and SSH, select this option. User Name and Password fields appear. Type the SSH User Name and Password. AccessIT logs into SSH using this User Name and Password.

10.3.8 VNC

Click **VNC**. The following are the default settings for VNC.



Settings > Access Services > VNC

Description: VNC

Application: vncviewer.exe

Port: 5900

Mode: ● VNC Client ○ Web

VNC application path: %ProgramFiles%\RealVNC

URL/Host:

Login Method: ○ Prompt for Credentials ● Use AccessIT Credentials ○ Use the Following Credentials

Figure 59 VNC – VNC Client mode

Windows/Linux tab – Select the operating system by clicking the appropriate tab. For each system the default VNC Application Path is different.

Description: - Description of the access service - VNC.

Application / VNC Application Path / Port – these fields are only relevant in VNC Client mode. The difference between VNC Client and Web mode is detailed below.

URL/Host: - Type the URL/Host of the VNC resource.

Mode: VNC Client (default)

When using VNC Client mode, the page appears as in see Figure 59.

VNC Client mode uses a VNC console server. In VNC Client the VNC application must be installed on all client computers, preferably in the same path. Type the path to the VNC Viewer application. Where the VNCPath is the actual installation folder of the VNC application, the installation folder depends on the type of VNC: RealVNC, TightVNC or UltraVNC. See the General notes above about variables.

The VNC application can be obtained from:

- RealVNC: http://www.realvnc.com
- TightVNC: http://www.tightvnc.com/
- UltraVNC: http://www.uvnc.com/

In VNC Client mode, the port number should correspond to the VNC listening port.

Login Method:

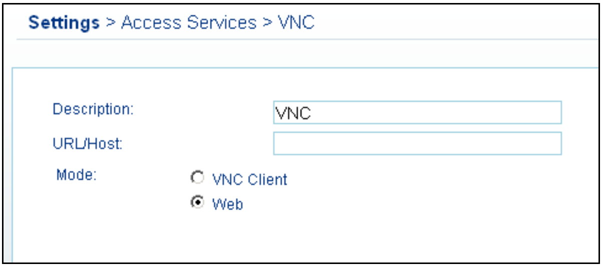
- Prompt for Credentials – this means the VNC login appears and you login manually.
- Use AccessIT Credentials – this means AccessIT logs into VNC with the currently logged user credentials. Ensure that VNC is configured to recognize the same password.
- Use the Following Credentials – Where the passwords are different for AccessIT and VNC, select this option. A Password field appears. Type the VNC Password. AccessIT logs into VNC using this Password.

Note! AccessIT fully supports the RealVNC Enterprise authentication method and uses a secured connection to the server. If free VNC editions are used, leave the username field blank and type the password where relevant.

Web mode

In Web mode there is no need for an executable application.

When selecting Web mode, the page appears as in Figure 60.



Settings > Access Services > VNC

Description: VNC

URL/Host:

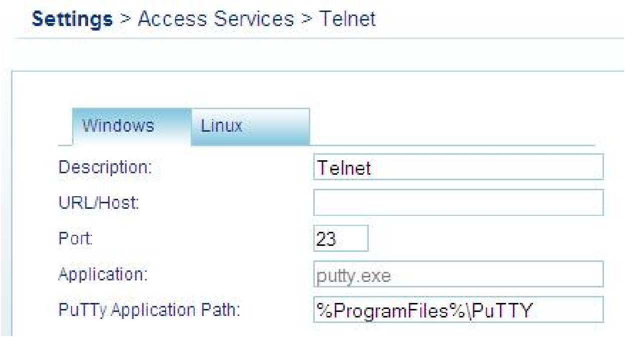
Mode: ○ VNC Client ● Web

Figure 60 VNC – Web mode

In Web mode there is only manual login.

10.3.9 Telnet

Click **Telnet**. The following are the default settings for Telnet.



Settings > Access Services > Telnet

Windows | Linux

Description: Telnet

URL/Host:

Port: 23

Application: putty.exe

PuTTy Application Path: %ProgramFiles%\PuTTY

Figure 61 Telnet

Windows/Linux tab – Select the operating system by clicking the appropriate tab. For each system the default PuTTy Application Path is different.

Description: - Description of the Access service - Telnet.

Application - PuTTy.exe is the application used for Telnet access. The PuTTy application can be obtained from: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

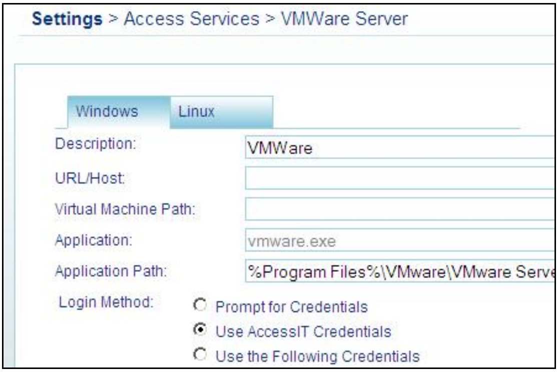
PuTTy Application Path: - - PuTTy application must be installed on all client computers, preferably in the same path. In the Windows default path %ProgramFiles%\PuTTy – see Figure 61 – the application could be in any drive in the Program Files\PuTTy folder. See the General notes above about variables.

URL/Host: - Type the URL/Host of the Telnet resource.

Port – The Telnet port number is 23 (default).

10.3.10 VMware Server

Click **VMware Server**. The following are the default settings for VMware Server.



Settings > Access Services > VMWare Server

Windows | Linux

Description: VMWare

URL/Host:

Virtual Machine Path:

Application: vmware.exe

Application Path: %Program Files%\VMware\VMware Serve

Login Method:
○ Prompt for Credentials
● Use AccessIT Credentials
○ Use the Following Credentials

Figure 62 VMware Server

Note! AccessIT built-in VMware server supports VMware server 1.x only. See the KVM.net II support website for VMware server 2.x and ESX Access Services.

Windows/Linux tab – Select the operating system by clicking the appropriate tab. For each system the default VMware Application Path is different.

Description: - Description of the access service - VMware Server.

Virtual Server Host or IP: - Type the Host/IP of the VMware Server resource.

Application - vmware.exe is the application used for VMware Server access. The VMware Server Client application can be obtained from:

http://www.vmware.com/download/server/

Application Path: - VMware Server console must be installed on all client computers, preferably in the same path. In the Windows default path %ProgramFiles%\VMware\VMware Server Console – see Figure 62 – the application could be in any drive in the Program Files\VMware\VMware Server Console folder. See the General notes above about variables.

Virtual Machine Path - Type the Virtual Machine Path on the VMware Server.

Login Method:

- Prompt for Credentials – this means the VMware Server Console login appears and you login manually.
- Use AccessIT Credentials – this means AccessIT logs into VMware Server Console with the currently logged user credentials. Ensure that VMware Server is configured to recognize the same User Name and Password.
- Use the Following Credentials – Where the User Name and Password are different for AccessIT and VMware Server, select this option. User Name and Password fields appear. Type the VMware Server User Name and Password. AccessIT logs into VMware Server using this User Name and Password.

10.3.11 New Access Services

You can add other access services. If the new service has an executable application the application must be installed on all client computers, preferably in the same path.

Add new Access Services as follows:

1. From the **Access Services** page click . The **New Service** page appears, see Figure 63. This page is a template for configuring a new access service.

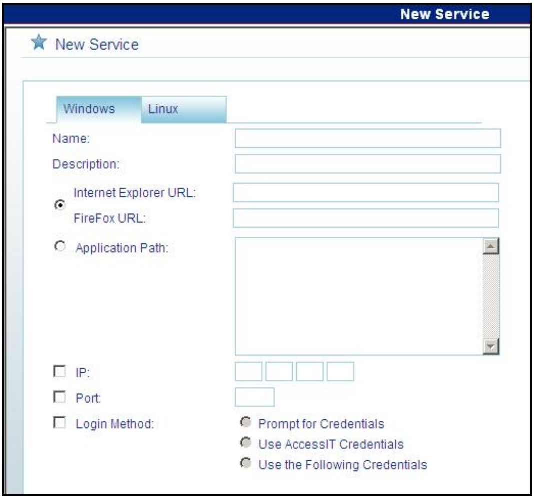


Figure 63 New Service page

Fill in the fields that are relevant to the service as follows:

Windows/Linux tab – Select the operating system by clicking the appropriate tab. For each system the default Application Path is different.

Name - Name of the Access service.

Description – Description of the access service.

URL – If the Access service resource can be reached via a web browser, type the URL here: HTTP or HTTPS etc. You may incorporate variables into the URL as follows:

- %ProgramFiles% - Program Files folder
- %SystemRoot% - Windows folder
- %IP% - IP address (**IP** checkbox must be selected)
- %Port% - TCP port number (**Port** checkbox must be selected)
- %UserName% - Login User name. A Login Method must be selected.
- %Password% - Login Password. **Login Method** checkbox must be selected.

Application Path – if the new service has an executable application the application must be installed on all client computers, preferably in the same path. The application could be in any drive in e.g. the following folder - %ProgramFiles%\Access service. Type the Application Path and executable name, including all command line switches, options and parameters.

IP – Type the IP address of the Access service resource.

Port – Where relevant, type the port number.

Login Method: If you need a login method choose from the following:

- Prompt for Credentials – this means the access service login appears and you login manually.
- Use AccessIT Credentials – this means AccessIT logs into the access service with the currently logged user credentials. Ensure that the access service is configured to recognize the same User Name and/or Password.
- Use the Following Credentials – Where the User Name and Password are different for AccessIT and the access service, select this option. User Name and Password fields appear. Type the access service User Name and/or Password. AccessIT logs into the access service using this User Name and/or Password.

Save the new service. The new service appears on the Access Services page.

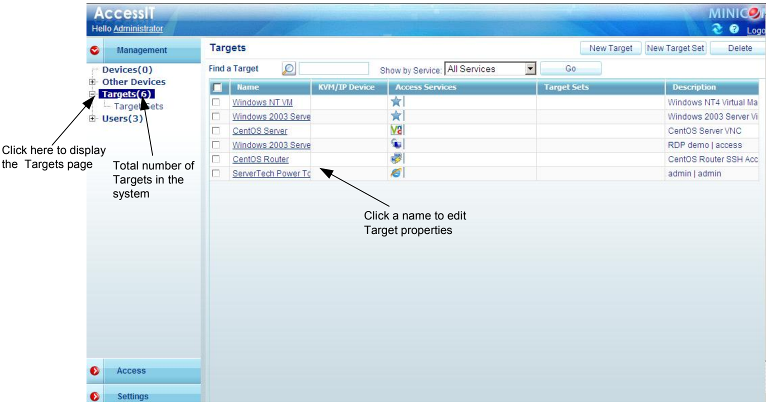
Note! See the KVM.net II support website for more information explaining how to create and configure additional Access Services.

11. Configuring Access services for individual Targets

As explained in section 10.3, the Access service default values are set globally in the Settings section of the menu – in **Applications/Access Services**. The following sections explain how to configure each Access service for individual Targets.

You configure the Access Services for each Target from the **Access Services** tab, as follows:

1. From the **Management** menu, select **Targets**, the **Targets** page appears see Figure 64.



☐	Name	KVM/IP Device	Access Services	Target Sets	Description
☐	Windows NT VM		★		Windows NT4 Virtual Ma
☐	Windows 2003 Serve		★		Windows 2003 Server Vi
☐	CentOS Server				CentOS Server VNC
☐	Windows 2003 Serve				RDP demo | access
☐	CentOS Router				CentOS Router SSH Acc
☐	ServerTech Power Tc				admin | admin

Click here to display the Targets page

Total number of Targets in the system

Click a name to edit Target properties

Figure 64 Target page

2. For new Targets click the **New Target** button, for existing Targets click the target name in the name column. The **Access Services** tab appears.

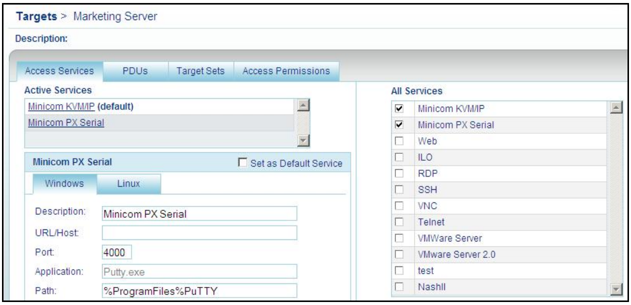
11.1 Default access service

You can set any of the access services to be the default service. This means that the service will be used to access the Target by default when selecting the Target name. To access the Target via a different service, the service must be selected. To set a service as the default, display the service as explained below and select the **Set as Default Service** checkbox.

11.2 Minicom PX Serial

To configure a Minicom PX Serial:

1. From the **All Services** list, select the **Minicom PX Serial** checkbox. Minicom PX Serial now appears in the **Active Services** list.
2. Click **Minicom PX Serial**. The Minicom PX Serial settings appear, see Figure 65.



Active Services:
- Minicom KVM/IP (default)
- Minicom PX Serial

Minicom PX Serial ☐ Set as Default Service

Description: Minicom PX Serial
URL/Host:
Port: 4000
Application: Putty.exe
Path: %ProgramFiles%PuTTY

All Services:
- ☑ Minicom KVM/IP
- ☑ Minicom PX Serial
- ☐ Web
- ☐ ILO
- ☐ RDP
- ☐ SSH
- ☐ VNC
- ☐ Telnet
- ☐ VMWare Server
- ☐ VMware Server 2.0
- ☐ test
- ☐ Nashll

Figure 65 Minicom PX Serial settings

Windows/Linux tab – Select the operating system by clicking the appropriate tab. For each system the default PuTTy Application Path is different.

Description: - Description of the access service - Minicom PX Serial.

Application: PuTTy.exe. This application must be installed on all client computers.

Path: - Path of the PuTTy application. Only change the default path if it is unsuitable.

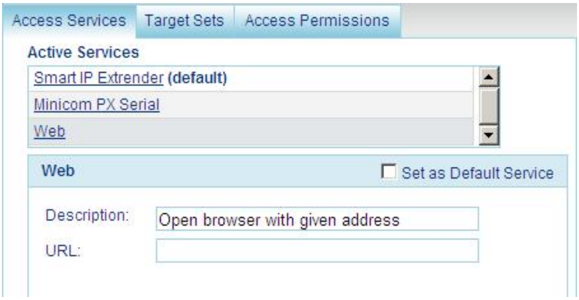
URL/Host: - Type the URL/Host of the Minicom PX Serial.

Port: - The Minicom PX Serial, TCP port number is 4000.

11.2.1 Web

From the **All Services** list, select the **Web** checkbox. Web appears in the **Active Services** list.

Click **Web**. The Web settings appear, see Figure 66.



Active Services:
- Smart IP Extrender (default)
- Minicom PX Serial
- Web

Web ☐ Set as Default Service

Description: Open browser with given address
URL:

Figure 66 Web Target

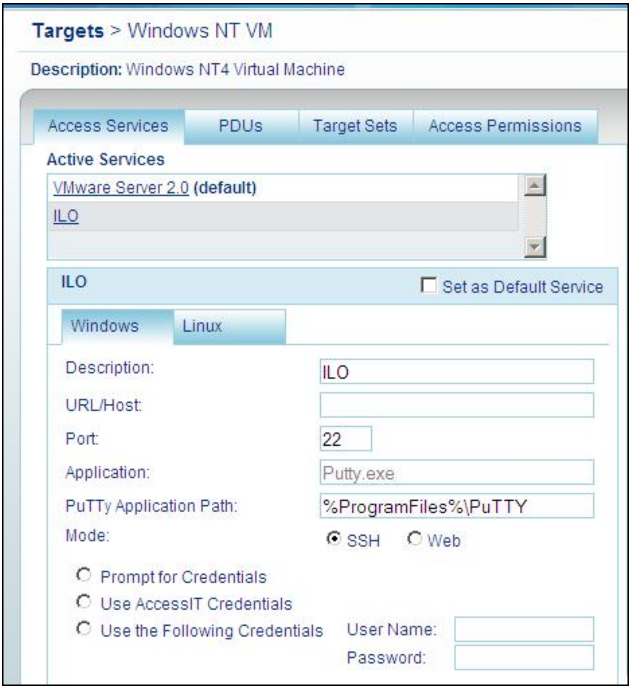
Description: - Description of the Web service.

URL: - Set the URL for each individual web page here.

11.2.2 ILO

From the **All Services** list, select the **ILO** checkbox. ILO appears in the Active **Services** list.

Click **ILO**. The ILO 2 settings appear, see Figure 67.



Targets > Windows NT VM

Description: Windows NT4 Virtual Machine

Active Services

- VMware Server 2.0 **(default)**
- ILO

ILO □ Set as Default Service

Description:	ILO
URL/Host:	
Port:	22
Application:	Putty.exe
PuTTy Application Path:	%ProgramFiles%\PuTTY
Mode:	● SSH ○ Web

○ Prompt for Credentials
○ Use AccessIT Credentials
○ Use the Following Credentials User Name: Password:

Figure 67 ILO

Windows/Linux tab – Select the operating system by clicking the appropriate tab. For each system the default PuTTy Application Path is different.

Description – Description of the access service - ILO.

URL/Host – Type the URL/Host of the ILO 2 resource.

Port / Application / PuTTy Application Path – these fields are only relevant in SSH mode. The difference between SSH and Web mode is detailed below.

SSH mode (default)

SSH mode uses an ILO 2 console server. In SSH mode the PuTTy application must be installed on all client computers, preferably in the same path. In the Windows default path %ProgramFiles%\PuTTy the application could be in any drive in the Program Files\PuTTy folder.

The PuTTy application can be obtained from:
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

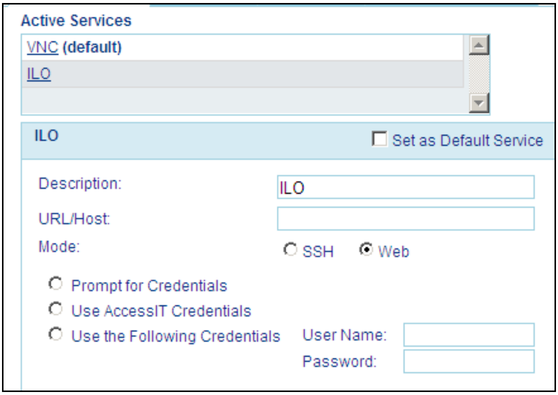
In SSH mode, the port number is 22 (default).

See below for Login method.

Web mode

Web mode uses a remote console with power management options. In Web mode there is no need for an executable application. Figure 55 illustrates the ILO 2 fields in Web mode.

Note! Automatic login in Web mode is supported in Internet Explorer only.



Active Services

VNC (default)

ILO

ILO □ Set as Default Service

Description: ILO

URL/Host:

Mode: ○ SSH ● Web

○ Prompt for Credentials

○ Use AccessIT Credentials

○ Use the Following Credentials User Name: Password:

Figure 68 ILO – Web mode

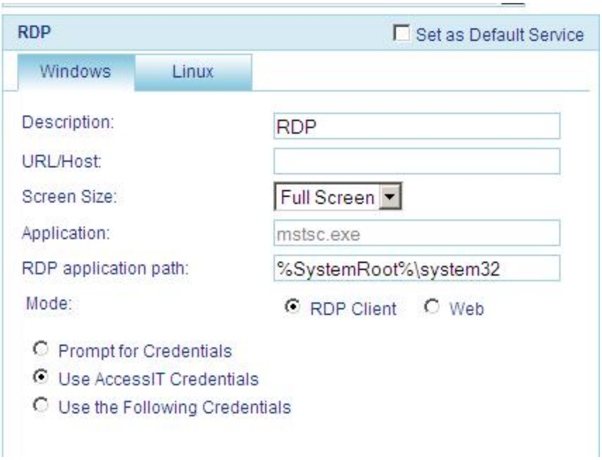
Login Method:

- Prompt for Credentials – This means the ILO 2 login appears and you login manually.
- Use AccessIT Credentials – This means AccessIT logs into ILO 2 with the currently logged user credentials. Ensure that ILO is configured to recognize the same username and password.
- Use the Following Credentials – Where the User Name and Password are different for AccessIT and ILO 2, select this option. User Name and Password fields appear. Type the ILO 2 User Name and Password. AccessIT logs into ILO 2 using this User Name and password.

11.2.3 RDP

From the **All Services** list, select the **RDP** checkbox. RDP appears in the Active **Services** list.

Click **RDP**. The RDP settings appear, see Figure 69.



RDP □ Set as Default Service

Description: RDP

URL/Host:

Screen Size: Full Screen

Application: mstsc.exe

RDP application path: %SystemRoot%\system32

Mode: ● RDP Client ○ Web

○ Prompt for Credentials

● Use AccessIT Credentials

○ Use the Following Credentials

Figure 69 RDP– RDP Client mode

Description: - Description of the access service - RDP.

URL/Host: - Type the URL/Host of the Target server.

Mode: - RDP Client or Web. These are explained below.

RDP Client mode (default)

RDP Client mode uses an RDP console server. From Windows XP onwards the executable application - mstsc.exe - comes as part of the operating system.

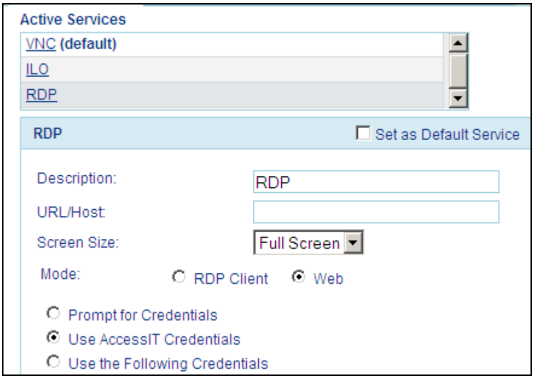
Windows/Linux tab – Select the operating system by clicking the appropriate tab. For each system the default RDP Application Path is different.

RDP Application Path: - The RDP application must be installed on all client computers, preferably in the same path. In the default path %SystemRoot%\System32 the application could be in any drive in the Windows\System32 folder.

Web mode

In Web mode there is no need for an executable application.

When selecting Web mode, the page appears as in Figure 70.



Active Services

VNC (default)

ILO

RDP

RDP ☐ Set as Default Service

Description: RDP

URL/Host:

Screen Size: Full Screen

Mode: ○ RDP Client ● Web

○ Prompt for Credentials

● Use AccessIT Credentials

○ Use the Following Credentials

Figure 70 RDP – Web mode

Screen Size: select the screen size from the drop-down menu.

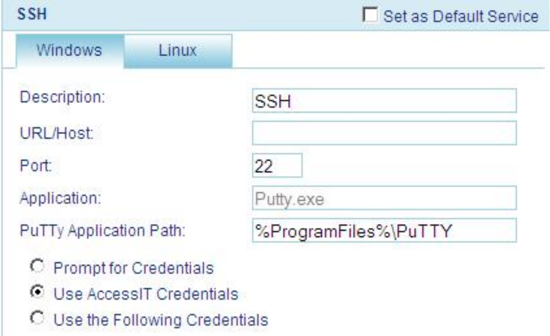
Login Method: -

- Prompt for Credentials – this means the RDP login appears and you login manually.
- Use AccessIT Credentials – this means AccessIT logs into RDP with the currently logged user credentials. Ensure that RDP is configured to recognize the same User Name and Password.
- Use the Following Credentials – Where the User Name and Password are different for AccessIT and RDP, select this option. User Name and Password fields appear. Type the RDP User Name and Password. AccessIT logs into RDP using this User Name and Password.

11.2.4 SSH

From the **All Services** list, select the **SSH** checkbox. SSH appears in the **Active Services** list.

Click **SSH**. The SSH settings appear, see Figure 71.



SSH ☐ Set as Default Service

Description: SSH

URL/Host:

Port: 22

Application: Putty.exe

PuTTy Application Path: %ProgramFiles%\PuTTY

○ Prompt for Credentials

● Use AccessIT Credentials

○ Use the Following Credentials

Figure 71 SSH

Windows/Linux tab – Select the operating system by clicking the appropriate tab. For each system the default PuTTy Application Path is different.

Description: - Description of the access service - SSH.

Application - PuTTy.exe is the application used for SSH access. The PuTTy application can be obtained from: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

PuTTy Application Path: - PuTTy application must be installed on all client computers, preferably in the same path. In the Windows default path %ProgramFiles%\PuTTy the application could be in any drive in the Program Files\PuTTy folder.

URL/Host: - Type the URL/Host of the SSH resource.

Port – The SSH port number is 22 (default).

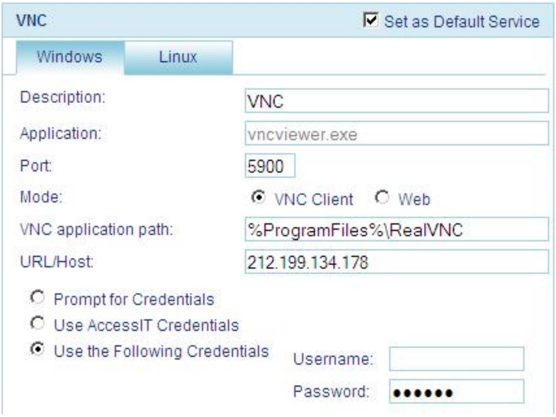
Login Method

- Prompt for Credentials – This means the SSH login appears and you login manually.
- Use AccessIT Credentials – This means AccessIT logs into SSH with the currently logged user credentials. Ensure that SSH is configured to recognize the same User Name and Password.
- Use the Following Credentials – Where the username and password are different for AccessIT and SSH, select this option. User Name and Password fields appear. Type the SSH User Name and Password. AccessIT logs into SSH using this User Name and Password.

11.2.5 VNC

From the **All Services** list, select the **VNC** checkbox. VNC appears in the Active Services list.

Click **VNC**. The VNC settings appear, see Figure 72.



VNC ☑ Set as Default Service

Description: VNC

Application: vncviewer.exe

Port: 5900

Mode: ● VNC Client ○ Web

VNC application path: %ProgramFiles%\RealVNC

URL/Host: 212.199.134.178

○ Prompt for Credentials

○ Use AccessIT Credentials

● Use the Following Credentials Username: Password: ••••••

Figure 72 VNC - VNC Client

Windows/Linux tab – Select the operating system by clicking the appropriate tab. For each system the default VNC Application Path is different.

Description: - Description of the access service - VNC.

Application / VNC Application Path / Port – these fields are only relevant in VNC Client mode. The difference between VNC Client and Web mode is detailed below.

URL/Host: - Type the URL/Host of the VNC resource.

Mode: VNC Client (default)

When using VNC Client mode, the page appears as in Figure 72.

VNC Client mode uses a VNC console server. In VNC Client the VNC application must be installed on all client computers, preferably in the same path. In the Windows default path %ProgramFiles%\VNCPath, the application could be in any drive in the Program Files\VNCPath folder, where the VNCPath is the actual installation folder of the VNC application. The installation folder depends on the type of VNC: RealVNC, TightVNC or UltraVNC.

The VNC application can be obtained from:

- RealVNC: http://www.realvnc.com
- TightVNC: http://www.tightvnc.com/
- UltraVNC: http://www.uvnc.com/

In VNC Client mode, the port number should correspond to the VNC listening port.

Login Method:

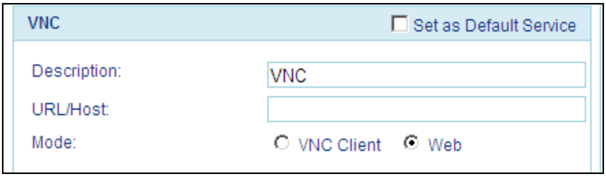
- Prompt for Credentials – this means the VNC login appears and you login manually.
- Use AccessIT Credentials – this means AccessIT logs into VNC with the currently logged user credentials. Ensure that VNC is configured to recognize the same username + password.
- Use the Following Credentials – Where the User Name and Password are different for AccessIT and VNC, select this option. User Name and Password field appears. Type the VNC the User Name and Password. AccessIT logs into VNC using this Password.

Note! AccessIT fully supports the RealVNC Enterprise authentication method and uses a secured connection to the server. If free VNC editions are used, leave the username field blank and type the password where relevant.

Web mode

In Web mode there is no need for an executable application.

When selecting Web mode, the page appears as in Figure 73.



VNC ☐ Set as Default Service

Description: VNC

URL/Host:

Mode: ○ VNC Client ● Web

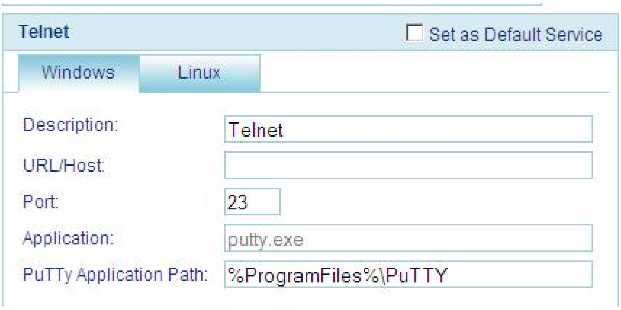
Figure 73 VNC – Web mode

In Web mode there is only manual login

11.2.6 Telnet

From the **All Services** list, select the **Telnet** checkbox. Telnet appears in the **Active Services** list.

Click **Telnet**. The Telnet settings appear, see Figure 74.



Telnet

□ Set as Default Service

Description: Telnet

URL/Host:

Port: 23

Application: putty.exe

PuTTy Application Path: %ProgramFiles%\PuTTY

Figure 74 Telnet

Windows/Linux tab – Select the operating system by clicking the appropriate tab. For each system the default PuTTy Application Path is different.

Description: - Description of the Access service - Telnet.

Application - PuTTy.exe is the application used for Telnet access. The PuTTy application can be obtained from:
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

PuTTy Application Path: - - PuTTy application must be installed on all client computers, preferably in the same path. In the default path %ProgramFiles%\PuTTy the application could be in any drive in the Program Files\PuTTy folder. See the General notes above about variables.

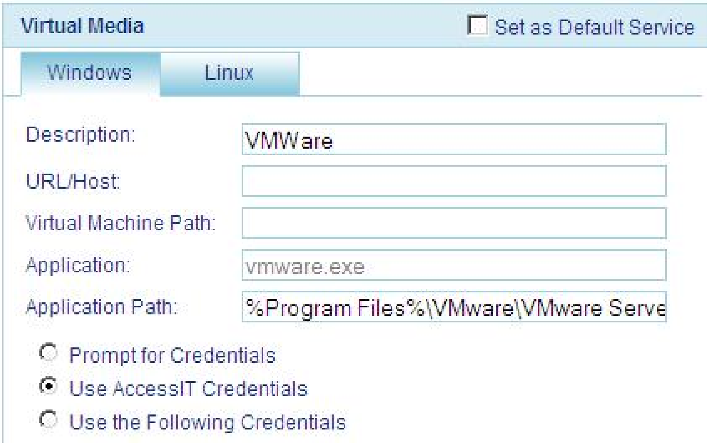
URL/Host: - Type the URL/Host of the Telnet resource.

Port – The Telnet port number is 23 (default).

11.2.7 VMware Server

From the **All Services** list, select the **VMware Server** checkbox. VMware Server 1.x appears in the **Active Services** list.

Click **VMware Server**. The VMware Server 1.x settings appear, see Figure 75.



Virtual Media □ Set as Default Service

Description: VMWare

URL/Host:

Virtual Machine Path:

Application: vmware.exe

Application Path: %Program Files%\VMware\VMware Serve

○ Prompt for Credentials

● Use AccessIT Credentials

○ Use the Following Credentials

Figure 75 VMware Server

Windows/Linux tab – Select the operating system by clicking the appropriate tab. For each system the default VMware Application Path is different.

Description: - Description of the access service - VMware Server.

Virtual Server Host or IP: - Type the Host/IP of the VMware Server resource.

Application - vmware.exe is the application used for VMware Server access. The VMware Server Client application can be obtained from:

http://www.vmware.com/download/server/

Application Path: - VMware Server console must be installed on all local computers, preferably in the same path. In the Windows default path %ProgramFiles%\VMware\VMware Server Console, the application could be in any drive in the Program Files\VMware\VMware Server Console folder.

Virtual Machine Path - Type the Virtual Machine Path on the VMware Server.

Login Method:

- Prompt for Credentials – this means the VMware Server login appears and you login manually.

- Use AccessIT Credentials – this means AccessIT logs into VMware Server Console with the currently logged user credentials. Ensure that VMware Server is configured to recognize the same username and password.
- Use the Following Credentials – Where the username and password are different for AccessIT and VMware Server, select this option. User Name and Password fields appear. Type the VMware Server User Name and Password. AccessIT logs into VMware Server using this User Name and Password.

Note! AccessIT built-in VMware server supports VMware server 1.x only. See the KVM.net II support website for VMware server 2.x and ESX Access Services.

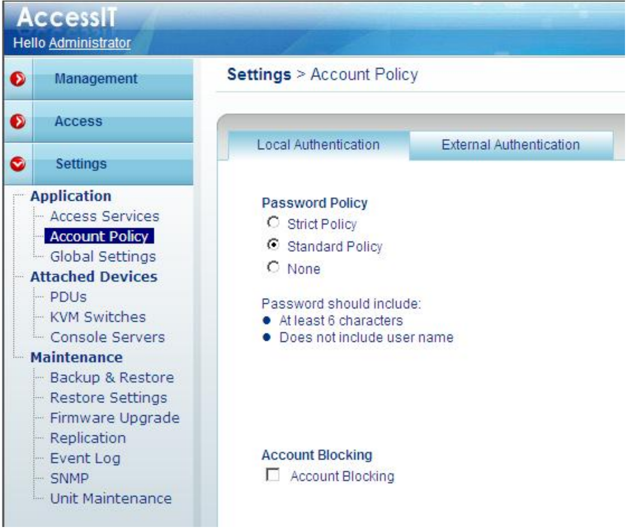
12. Account Policy

In **Account Policy** you can choose either local or external authentication. In local authentication you define password and login complexity levels. External authentication interfaces with the organizational Active Directory server for user list importation and user authentication.

In local authentication mode the administrator creates Users and Groups and assigns permissions via the AccessIT interface. In LDAP authentication mode, user authentication is done through an LDAP server. You import Users and Groups from the LDAP server and assign their permissions in the AccessIT interface.

To set these options:

From the **Application** menu select **Account Policy**. The Account policy page appears, see Figure 76.



Password Policy

○ Strict Policy

● Standard Policy

○ None

Password should include:

- At least 6 characters
- Does not include user name

Account Blocking

□ Account Blocking

Figure 76 Account policy

12.1 Password policy

When AccessIT operates in local authentication mode, choose the desired password policy. The different password policy options are explained below.

Note! The following “special” characters: &, <, >, ”, cannot be used for either the user name or password in any of the password levels. (See page 22).

Strict Policy password:

- 8 characters or more
- Must include at least

  - 1 digit and
  - 1 upper case letter and
  - 1 “special” character as follows: !.@#$%^ *( )_-+= [ ]{ }
- Must not include the user name

Standard Policy password:

- 6 characters or more
- Must not include the user name

None:

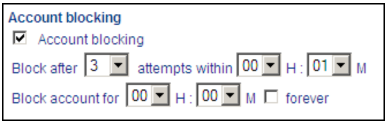
You can write any character (except the “special” characters: &, <, >, ”,) and any number of characters for the password. (See page 22).

12.1.1 Account blocking

You can block entry into the system after a number of unsuccessful attempts by a user inputting the wrong password.

To do so:

1. Select the **Account blocking** checkbox. The following appears.



Account blocking

☑ Account blocking

Block after 3 attempts within 00 H : 01 M

Block account for 00 H : 00 M □ forever

Figure 77 Account blocking

Choose the number of attempts within a time period and for how long to block the account for.

12.2 External authentication (LDAP)

LDAP, (Lightweight Directory Access Protocol), is a standard protocol for accessing information in a directory.

LDAP defines processes by which a client can connect to an X.500-compliant or LDAP-compliant directory service to add, delete, modify, or search for information, provided the client has sufficient access rights to the directory. For example, a user could use an LDAP client to query a directory server on the network for information about specific users, computers, departments, or any other information stored in the directory.

Note! AccessIT supports Windows 2003 and Windows 2008 Active Directory LDAP Authentication.

12.2.1 AccessIT in External authentication (LDAP) mode

In External authentication (LDAP) mode, AccessIT deletes all users created before in Local authentication mode. New users can only be imported from a Windows 2003 or Windows 2008 Active Directory.

AccessIT will validate all user credentials against the external LDAP server only.

Only the “admin” account remains as a “backdoor” account. This user has AccessIT local access. Admin account is allowed to manage AccessIT with "Administrator" access privileges. However, "admin" is not permitted to connect to Targets. This account will allow changing AccessIT to Local authentication mode at any time.

There is no direct access to any IP device. AccessIT will act as a gateway.

Since the AccessIT user accounts are kept in the local database, it can happen that some of the local accounts do not have related LDAP objects (e.g. some user's account might migrate to another LDAP path). To clean the local database from those ghost accounts that will never pass LDAP authentication, AccessIT provides the customers with the manual synchronize operation.

Users Groups will not be deleted and will be managed locally after its import.

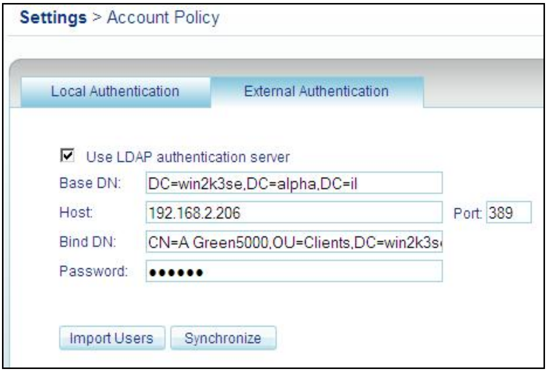
When changing AccessIT to Local authentication mode, all the users appear as “inactive”. To re-activate the users, the Administrator must explicitly provide each account with a local password.

12.2.2 DNS setting in LDAP mode

Important! The correct DNS setting is vital for the successful configuration of the AccessIT in LDAP mode. You set the AccessIT DNS settings in the Settings / Unit Maintenance / Network tab. See section 16.2 on page 106.

12.2.3 LDAP settings

1. Select the **External Authentication** tab, the LDAP settings appears, see Figure 78.



Settings > Account Policy

☑ Use LDAP authentication server

Base DN: DC=win2k3se,DC=alpha,DC=il

Host: 192.168.2.206 Port: 389

Bind DN: CN=A Green5000,OU=Clients,DC=win2k3s

Password: ●●●●●●

Figure 78 LDAP settings

2. Select the **Use LDAP authentication server** checkbox.
3. Input details of the Active Directory:

Base DN – here you define the base object where the search for users begins. The search is performed only on this object and the objects below it in the directory tree. The Base DN string has the standard LDAP syntax: CN=(Common Name…), OU=(Organizational Unit), DC=(Domain Component). Base DN should be in the following format **DC=domain,DC=tld**. For example for the domain KVM.net.org, the Base DN should be **DC=kvm,DC=net,DC=org**.

Host – Type the Host name or (preferably) the IP address of the Active Directory DC server.

Port - Type the LDAP port number. If left blank; AccessIT uses the default LDAP port 389 (which is the default port for most LDAP servers including Microsoft Active Directory).

Bind DN – Also known as "User DN" or "Append". The Bind DN is a distinguished name of an LDAP object, which serves a gateway to the LDAP directory. Prior to sending the account/password pair, AccessIT initiates a conversation handshake with LDAP. This handshake protocol in general needs a "Bind DN/Bind password" pair to decide, whether the AccessIT client is permitted to query the LDAP directory server. (For example if we have user Minicom in group Users in domain KVM.net.org the Bind DN should look like this: **CN=minicom,CN=users,DC=kvm,DC=net,DC=org**).

Type the Active Directory objects you would like to search and the user account that will be used to perform this operation.

Password – Type the password for the user account given in the Bind DN.

4. Click Save. The system queries the Active Directory. (This may take some time). The Import Users and Synchronize buttons become enabled.

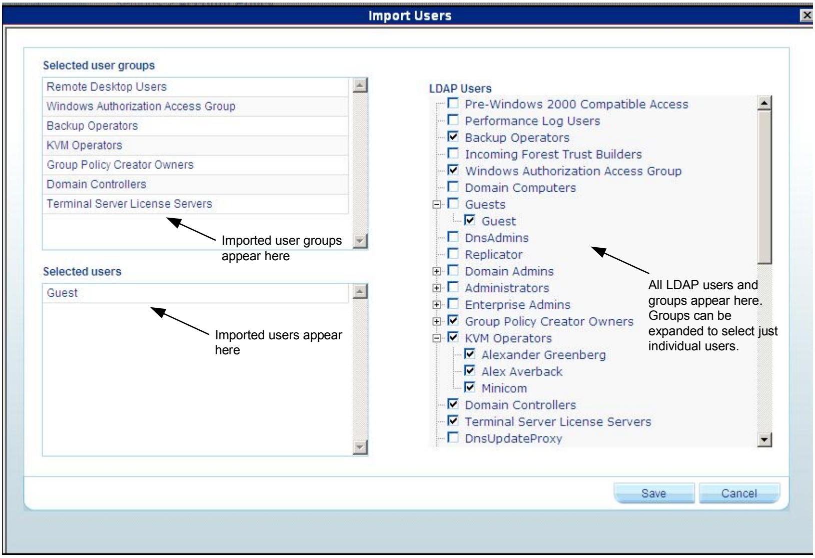
12.2.4 Importing users

To import users, press Import Users, the Import Users window appears, see Figure 79. Here you see all the Groups in the Active Directory.

To display the Users in a directory, expand the Group.

Notes:

- Users must be members of groups in order to be shown in the Import Users Active Directory tree. Users belonging to the container "Users" in the Active Directory, do not necessarily belong to any Group.
- You can use the Active Directory command "dsquery user" to list all Active Directory users with their correct Bind DN parameters. Run "dsquery user" at the command prompt of your Active Directory Domain Contoller.



Selected user groups

Remote Desktop Users
Windows Authorization Access Group
Backup Operators
KVM Operators
Group Policy Creator Owners
Domain Controllers
Terminal Server License Servers

Imported user groups appear here

Selected users

Guest

Imported users appear here

LDAP Users

- □ Pre-Windows 2000 Compatible Access
- □ Performance Log Users
- ☑ Backup Operators
- □ Incoming Forest Trust Builders
- ☑ Windows Authorization Access Group
- □ Domain Computers
- □ Guests
  - ☑ Guest
- □ DnsAdmins
- □ Replicator
- □ Domain Admins
- □ Administrators
- □ Enterprise Admins
- ☑ Group Policy Creator Owners
- ☑ KVM Operators
  - ☑ Alexander Greenberg
  - ☑ Alex Averback
  - ☑ Minicom
- ☑ Domain Controllers
- ☑ Terminal Server License Servers
- □ DnsUpdateProxy

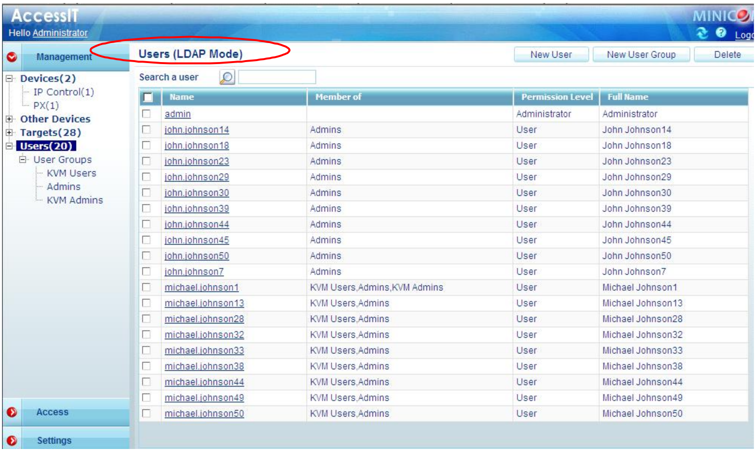
All LDAP users and groups appear here. Groups can be expanded to select just individual users.

Figure 79 Import LDAP Users window

You can import:

- A Group with all its users by selecting the Group.
- Some users of a Group by expanding the Group and then selecting the desired users.

Once selected, the Groups and Users appear in the **Selected User Group/User** area. Press **Save**, the Groups and Users appear in the Users/Groups section of the AccessIT, with the words “Users (LDAP mode)” at the top of the page, see Figure 80.



Users (LDAP Mode)

□	Name	Member of	Permission Level	Full Name
□	admin		Administrator	Administrator
□	john.johnson14	Admins	User	John Johnson14
□	john.johnson18	Admins	User	John Johnson18
□	john.johnson23	Admins	User	John Johnson23
□	john.johnson29	Admins	User	John Johnson29
□	john.johnson30	Admins	User	John Johnson30
□	john.johnson39	Admins	User	John Johnson39
□	john.johnson44	Admins	User	John Johnson44
□	john.johnson45	Admins	User	John Johnson45
□	john.johnson50	Admins	User	John Johnson50
□	john.johnson7	Admins	User	John Johnson7
□	michael.johnson1	KVM Users,Admins,KVM Admins	User	Michael Johnson1
□	michael.johnson13	KVM Users,Admins	User	Michael Johnson13
□	michael.johnson28	KVM Users,Admins	User	Michael Johnson28
□	michael.johnson32	KVM Users,Admins	User	Michael Johnson32
□	michael.johnson33	KVM Users,Admins	User	Michael Johnson33
□	michael.johnson38	KVM Users,Admins	User	Michael Johnson38
□	michael.johnson44	KVM Users,Admins	User	Michael Johnson44
□	michael.johnson49	KVM Users,Admins	User	Michael Johnson49
□	michael.johnson50	KVM Users,Admins	User	Michael Johnson50

Figure 80 Users (LDAP mode)

If the number of users in the imported group exceeds the number of users supported by AccessIT (up to 20), a warning message appears and only the first 19 users are imported from the LDAP server. (The user ‘admin’ always remains in the system).

After importing Users, you must assign their permissions - Administrator or User. How to assign permissions is explained in section 6 on page 21. By default all imported users have User permission status. (Also assign their Target permissions and allowed Access Services).

12.2.5 Synchronization

Synchronization does two things:

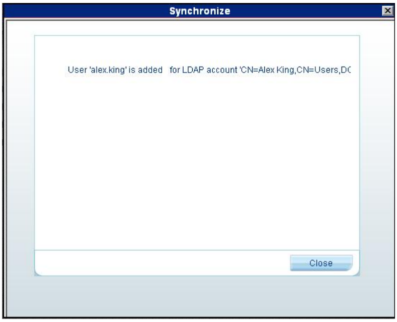
- Keeps the exact group structure maintained on the LDAP servers. (Whenever a user is added or removed from the LDAP server group, it will be synchronized with the AccessIT).
- Removes deleted users. A user that resides in AccessIT but is deleted from the LDAP server will be removed from AccessIT as well.

Where users and/or Groups have been added or deleted from the LDAP database, you can synchronize the local user database with the LDAP database. There is no need to import new users from the LDAP database, synchronization does this automatically, provided that the new user is added to one of the groups imported into the AccessIT.

To synchronize:

Click Synchronize. The local user database is compared to the LDAP database. Any local user that does not exist on the LDAP server is noted as deleted. Any new user added to already imported AccessIT Groups in the LDAP database is noted as added, see Figure 81.

Note: To add a user to the AccessIT Groups using the synchronize function, add this user to the imported Group in the LDAP server.



User 'alex.king' is added for LDAP account 'CN=Alex King,CN=Users,DC

Figure 81 Synchronize window

12.2.6 Operating AccessIT in External Authentication mode

In External Authentication (LDAP) Mode, AccessIT Manager will no longer allow login for the users that were created in Local Authentication mode. These users will be deleted. New users will be imported from Active Directory.

AccessIT Manager will validate all user credentials against the LDAP server only.

Only the “admin” account retains local authentication as a “backdoor” account. This user has AccessIT local access. Admin account is allowed to manage AccessIT with "Administrator" access privileges. However, "admin" is not permitted to connect to Targets. This account will allow reversing the External Authentication Mode at any time to local authentication mode.

There is no direct access to any IP device, even to its Configuration page. AccessIT will act as a gateway.

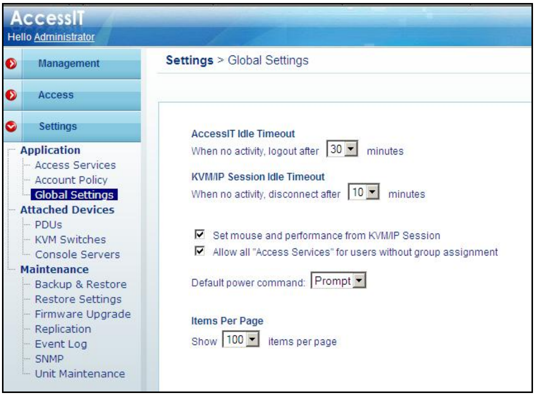
When changing AccessIT to Local Authentication mode, all imported users appear as “inactive”. To re-activate the users, the administrator must set a password for each account.

Clicking the **New User** button on the Users page - see page 21 - opens the **Import LDAP Users** window.

13. Global Settings

In Global Settings, you can change the idle timeout period and set out global parameters as explained below.

From the menu click **Global Settings**, the following appears.



AccessIT Idle Timeout
When no activity, logout after 30 minutes

KVM/IP Session Idle Timeout
When no activity, disconnect after 10 minutes

☑ Set mouse and performance from KVM/IP Session
☑ Allow all "Access Services" for users without group assignment

Default power command: Prompt

Items Per Page
Show 100 items per page

Figure 82 Global Settings

13.1 AccessIT / KVM/IP Session Idle timeout

Select the number of minutes of non-activity, after which the AccessIT and KVM/IP sessions will terminate. The User will then have to re-login.

Set mouse and performance from KVM/IP Session

This checkbox determines who updates the local mouse and performance settings. When checked, local mouse and performance settings are determined at the remote session level. Unselecting this option will apply defaults settings to all devices. In order to change the settings the administrator must configure each device separately.

By selecting the checkbox AccessIT will not overwrite local mouse and performance settings made in the client toolbar.

Allow all "Access Services" for users without group assignment

For users not assigned to any user groups select the checkbox to allow all "Access Services" by default. Unselecting this option prevents access to any service for individual users that don't belong to any group, including administrators.

Default power command

For power management devices you can select the Default power command from the drop-down list. Choose Prompt, On, Off or Cycle. The chosen command will be the default sent to the connected device.

Items Per Page

Select the maximum number of items – Targets, Groups etc – to appear on one page. When this number is reached additional items are put on another page. You click on the page link to open the next page.

Click **Save** to save changes.

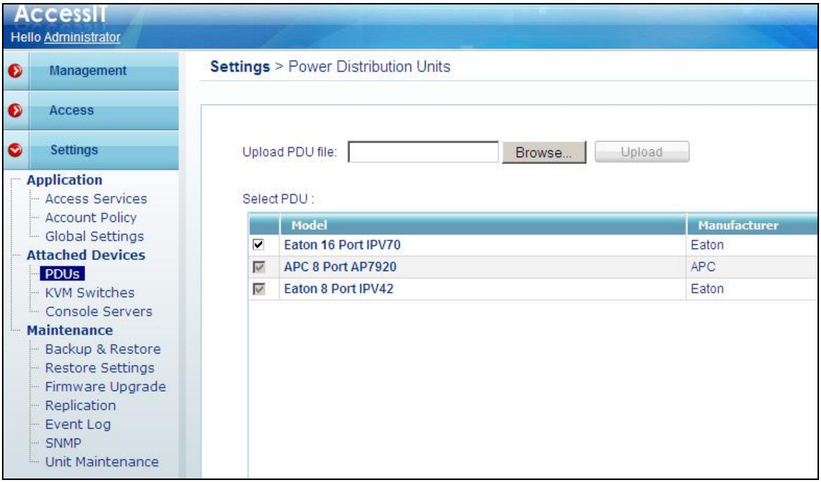
14. Attached Devices

Attached Devices refers to Power Distribution Units (PDU), KVM switches and Console servers physically connected to the system's Targets. You must select the devices attached to the system.

14.1 Selecting PDUs

To select a PDU type:

1. From the **Settings/Attached Devices** menu, select **PDU,** the **PDU** page appears showing a list of PDU types, see Figure 83.



Settings > Power Distribution Units

Upload PDU file:

Select PDU :

	Model	Manufacturer
☑	Eaton 16 Port IPV70	Eaton
☑	APC 8 Port AP7920	APC
☑	Eaton 8 Port IPV42	Eaton

Figure 83 PDU page

The columns show the following:

- **Model** - PDU model
- **Manufacturer** - PDU manufacturer

2. From the list, select the PDU brands and models physically connected to your Targets.

3. Press Save. The selection is saved. The PDU appears in the management section in the drop-down list of PDUs (see page 49).

14.1.1 Uploading a new PDU model

If a PDU is not listed, contact Minicom at support@minicom.com to obtain a new PDU definition file.

When you receive the file do the following:

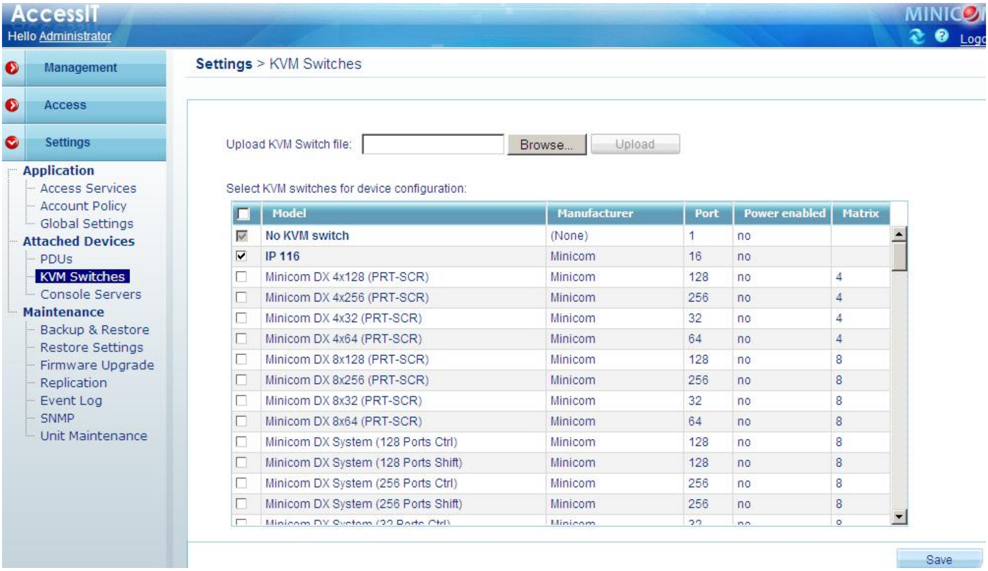
1. Save the PDU file on your computer’s hard disk.
2. Login to AccessIT as an Administrator.
3. From the **PDU** page - see Figure 83 - press Browse... to locate the Figure 83 file (PDU.XML).
4. Press Upload. The file uploads with the new PDU type added to the list.
5. Select the PDU type and click Save. The PDU appears in the management section in the drop-down list of PDUs (see page 49).

14.2 KVM switches

Configuring KVM switches is relevant when there are KVM switches connected to IP devices in the system or when there are DXU IP II units in the system. You must select all the KVM switch types physically connected.

To select the KVM switch types:

1. From the **Settings/Attached Devices** menu, select **KVM Switches.** A list of KVM switches appears, see Figure 84. The columns show the following:
   - **Model** - KVM switch model
   - **Manufacturer** - KVM switch manufacturer
   - **Ports** - The number of server ports
   - **Power Enabled -** Power enabled status. Where the KVM switch is connected to a power management device such as a Minicom Remote Power Switch or Power on Cable, the status of this column is **yes** meaning it is power enabled. **No** means it is not enabled.
   - **Matrix** – The number of simultaneous users this switch supports. **Note!** Where you know a KVM switch has matrix capabilities, but no number appears in the **Matrix** column, contact the Minicom Support team to obtain the updated SDF of the KVM switch. Uploading the SDF is explained in section 14.2.1 below.



Settings > KVM Switches

Upload KVM Switch file:

Select KVM switches for device configuration:

□	Model	Manufacturer	Port	Power enabled	Matrix
☑	No KVM switch	(None)	1	no	
☑	IP 116	Minicom	16	no	
□	Minicom DX 4x128 (PRT-SCR)	Minicom	128	no	4
□	Minicom DX 4x256 (PRT-SCR)	Minicom	256	no	4
□	Minicom DX 4x32 (PRT-SCR)	Minicom	32	no	4
□	Minicom DX 4x64 (PRT-SCR)	Minicom	64	no	4
□	Minicom DX 8x128 (PRT-SCR)	Minicom	128	no	8
□	Minicom DX 8x256 (PRT-SCR)	Minicom	256	no	8
□	Minicom DX 8x32 (PRT-SCR)	Minicom	32	no	8
□	Minicom DX 8x64 (PRT-SCR)	Minicom	64	no	8
□	Minicom DX System (128 Ports Ctrl)	Minicom	128	no	8
□	Minicom DX System (128 Ports Shift)	Minicom	128	no	8
□	Minicom DX System (256 Ports Ctrl)	Minicom	256	no	8
□	Minicom DX System (256 Ports Shift)	Minicom	256	no	8
□	Minicom DX System (32 Ports Ctrl)	Minicom	32	no	8

Figure 84 KVM Switches

2. From the list, select the KVM switch brands and models physically connected to your IP devices. When there are Smart 116 IP units in the system, select **IP 116** from the list.

When there are DXU IP II units in the system:

For **enabled** mode, select the correct DX configuration with **Ctrl** (and not PRT-SCR hotkey). For example when there is 1 DX Central unit in the DX system, select **Minicom DX System (32 ports Ctrl)**. When there are 2 DX Central units in the DX system select **Minicom DX System (64 ports Ctrl)**.

For **managed** mode, select the correct DX configuration with **PRT-SCR** (and not Ctrl hotkey). For example when there is 1 DX 432 Central unit in the DX system, select **Minicom DX4x32 (PRT-SCR)**. When there are two 832 DX Central units in the DX system select **Minicom DX8x64 (PRT-SCR)**.

3. Press Save. The selection is saved.

14.2.1 Uploading a new KVM Switch

If a KVM switch is not listed, contact Minicom at support@minicom.com to obtain a new KVM switch definition file (SDF).

When you receive the file do the following:

1. Save the KVM switch file on your computer's hard disk.
2. Login to AccessIT as an Administrator.

3. From the **KVM Switches** page - see Figure 84 - press Browse... to locate the KVM switch file (SDF.XML).

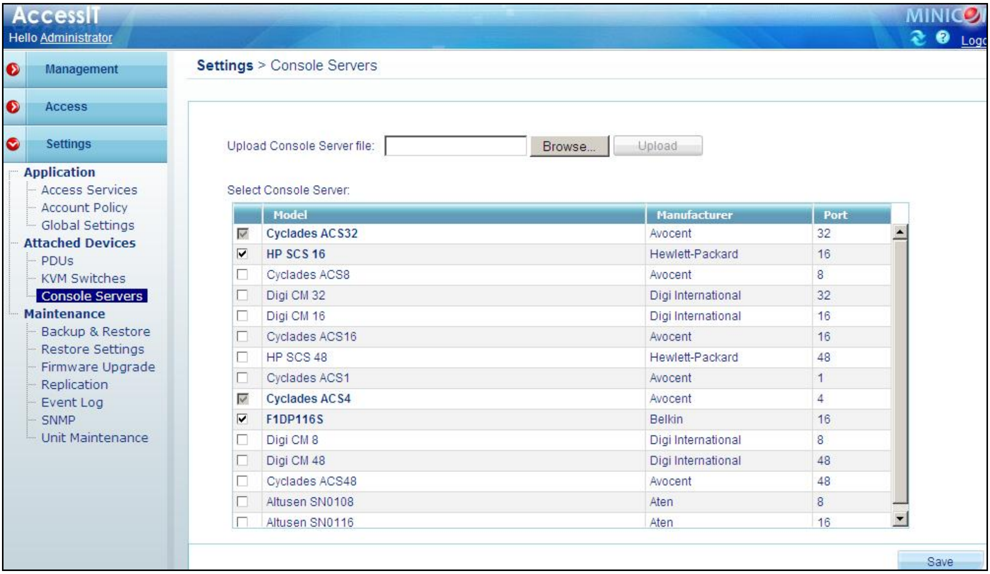
4. Press Upload. The file uploads with the new switch type added to the list.

5. Select the KVM switch type and click Save.

14.3 Configuring a Console server

To select a Console server type:

1. From the **Settings/Attached Devices** menu, select **Console Servers** the **Console Servers** page appears showing a list of Console Servers, see Figure 85.



Upload Console Server file:

Select Console Server:

	Model	Manufacturer	Port
☑	Cyclades ACS32	Avocent	32
☑	HP SCS 16	Hewlett-Packard	16
□	Cyclades ACS8	Avocent	8
□	Digi CM 32	Digi International	32
□	Digi CM 16	Digi International	16
□	Cyclades ACS16	Avocent	16
□	HP SCS 48	Hewlett-Packard	48
□	Cyclades ACS1	Avocent	1
☑	Cyclades ACS4	Avocent	4
☑	F1DP116S	Belkin	16
□	Digi CM 8	Digi International	8
□	Digi CM 48	Digi International	48
□	Cyclades ACS48	Avocent	48
□	Altusen SN0108	Aten	8
□	Altusen SN0116	Aten	16

Figure 85 Console Servers page

The columns show the following:

- **Model** - Console Server model
- **Manufacturer** - Console Server manufacturer
- **Port** – Number of ports on the Console Server

2. From the list, select the Console Server brands and models physically connected to your Targets.

3. Press Save. The selection is saved. The Console Server appears when configuring Console Servers in the Management section, in the drop-down list of Console Servers (see page 52).

14.3.1 Uploading a new Console Server model

If a Console Server is not listed, contact Minicom at support@minicom.com to obtain a new Serial Console definition file.

When you receive the file do the following:

1. Save the file on your computer's hard disk.
2. Login to AccessIT as an Administrator.
3. From the **Console Server** page - see Figure 85 - press Browse... to locate the file (SCDF.XML).
4. Press Upload. The file uploads with the new Serial Console type added to the list.

5.Select the Serial Console type and click Save. The Serial Console appears in the management section in the drop-down list of of Console Servers (see page 52).

15. System Maintenance

Maintenance includes the following:

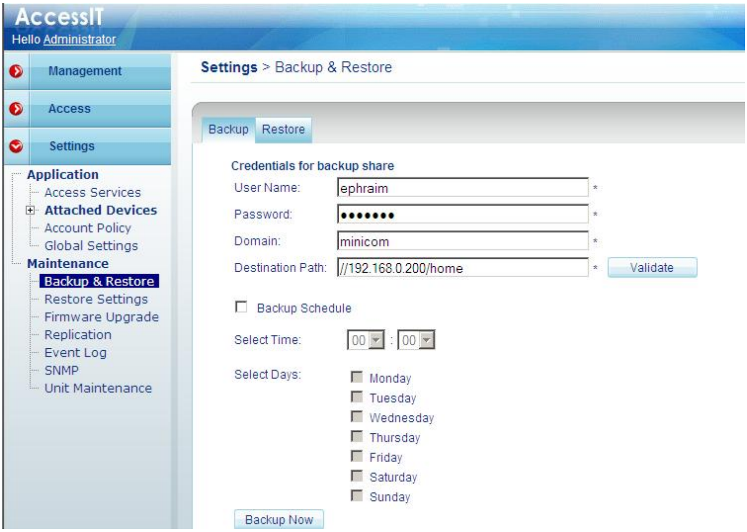
- Backup & Restore
- Restore Settings
- Firmware Upgrade
- Replication
- Event Log
- SNMP
- Unit Maintenance

15.1 Backup & Restore

You can set up an automatic backup schedule for the AccessIT Manager database.

To do so:

From the **Maintenance** menu click **Backup & Restore**, the **Backup** page appears, see Figure 86.



Credentials for backup share

User Name: ephraim *

Password: ••••••• *

Domain: minicom *

Destination Path: //192.168.0.200/home *

□ Backup Schedule

Select Time: 00 : 00

Select Days:
□ Monday
□ Tuesday
□ Wednesday
□ Thursday
□ Friday
□ Saturday
□ Sunday

Figure 86 Backup page

15.1.1 The backup elements

Credentials for backup share - Enter the user credentials (name, password, and domain) of the network share path to which the backup file will be saved. (The designated backup share must require both user and password login).

Destination path - enter the remote computer name and shared folder or its IP address and shared folder using the following path syntax:

//computer name/share - e.g. //gx270n-comp163/backup

or

//computer IP address/share - e.g. //192.168.2.71/backup

Note: Netware shares are not supported.

For computer name resolving the DNS server IP address must be set in the **Unit Maintenance/Network** tab.

To validate the Destination path, click Validate.

Backup schedule – Select the checkbox to activate the backup schedule.

Select time - Select the time (hour and minute) that the backup should initiate.

Select days - Select which days the backup should be performed.

Click Save to save the settings.

The scheduled times work according to the internal clock of the AccessIT Manager appliance.

To perform a manual backup at any time, click Backup Now. The Backup file is stored in the destination path.

15.1.2 Restoring database backup

To restore the AccessIT database from a previously created backup file:

1. Click the **Restore** tab, the following appears.

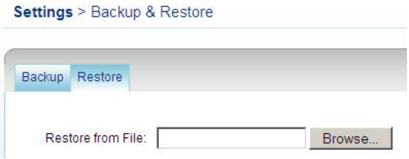


Figure 87 Restore tab

2. Browse to locate the backup file.
3. Load the backup file.
4. Click Restore. After the process finishes, you are logged out from the AccessIT web interface, login again. AccessIT system is ready to use.

15.2 Restore Settings

1. Click **Restore Settings**, the following appears.

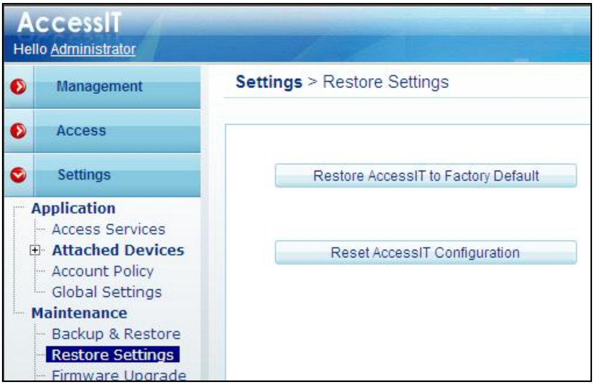


Figure 88 Restore Settings

From Restore Settings you can:

- Restore AccessIT to the factory default settings
- Reset all configurations without deleting the database entities.

15.2.1 Restoring AccessIT to factory default settings

To restore the AccessIT Manager to its factory default settings:

Click Restore AccessIT to Factory Default. A prompt appears notifying you that all database configurations will be lost. Click **OK**. AccessIT system restarts with the restored factory settings.

15.2.2 Resetting AccessIT configuration

You can reset all configurations without deleting the database entities. To do so:

Click Reset AccessIT Configuration. A prompt appears notifying you that all associations will be lost. Click **OK**. All associations are deleted.

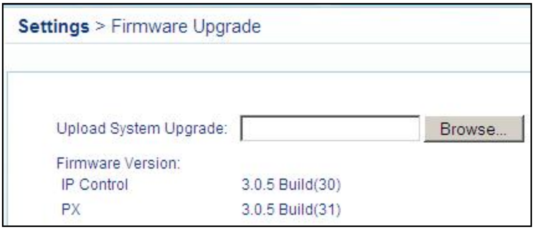
15.3 Firmware upgrade

Periodically Minicom releases firmware upgrades for its IP devices and the AccessIT Manager. These upgrades can be found at www.minicom.com in the Support section. Through the AccessIT Manager an Administrator can upgrade the firmware of the AccessIT Manager and all connected IP devices making it unnecessary to upgrade each device individually.

15.3.1 Upgrading the IP devices firmware

To upgrade the firmware version of all connected IP devices or the AccessIT Manager:

1. Obtain the latest firmware version from Minicom.
2. Save the file on the client computer.
3. Login to the AccessIT Manager Web interface.
4. From the **Settings/Maintenance** menu, click **Firmware Upgrade**, Figure 89 appears.



Settings > Firmware Upgrade

Upload System Upgrade: [ ] Browse...

Firmware Version:

IP Control 3.0.5 Build(30)

PX 3.0.5 Build(31)

Figure 89 Firmware upgrade

5. Press **Browse** and locate the upgrade file.
6. Press Start Upgrade. AccessIT loads the firmware and initiates the upgrade.

When upgrading IP devices the firmware uploads to 5 IP devices at a time – IP device status changes to **Uploading** and then to **Rebooting** as the firmware finishes upgrading (see page 39). The uploaded firmware is stored in the AccessIT Manager. Every new IP device connected to the system is automatically upgraded to this firmware.

15.3.2 Upgrading the AccessIT Manager

When upgrading the AccessIT Manager, the AccessIT Manager reboots automatically. Login again.

15.4 Replication

You can add a secondary AccessIT Manager unit to the system. The primary unit then replicates all data to the secondary unit. In the event of a failure in the primary unit, the secondary unit can take over, and operate with the most up to date database.

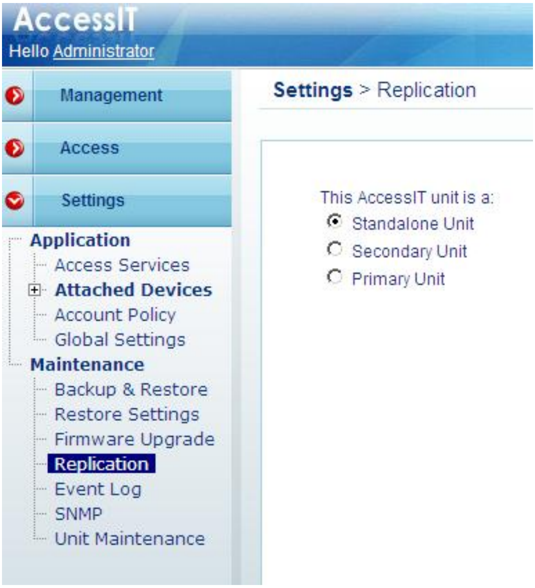
15.4.1 Connecting the secondary unit to the network

1. Connect the secondary unit to a power supply outlet.
2. Connect the secondary unit to the network as follows: On the rear panel connect an Ethernet cable to LAN 1
3. Power up the secondary unit.

15.4.2 Configuring the secondary unit

Configure the secondary unit before configuring the primary unit. Configuration involves changing the secondary unit IP address, (so as not to cause a network conflict by having the same IP address as the primary unit) and assigning the unit to be the secondary unit.

1. From the secondary unit login to the AccessIT Manager web interface. See section 5 on page 19 to display the AccessIT Web interface.
2. Change the IP address of the secondary unit to be different to the primary unit, but ensure that it resides on the same network segment. You change the secondary unit IP address from the **Network** tab under **Settings**/**Unit Maintenance**. See section 16.2 on page 106. Once changed, the unit restarts.
3. Login again with the new network settings.
4. From the **Settings**/**Maintenance** menu, click **Replication**, Figure 90 appears.



This AccessIT unit is a:

● Standalone Unit

○ Secondary Unit

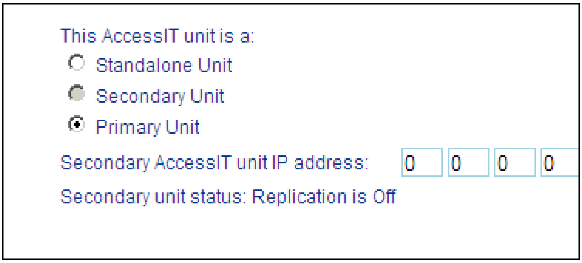
○ Primary Unit

Figure 90 Replication page

5. Select **Secondary Unit**. A field for the IP address of the primary unit appears.
6. Type the primary unit IP address.
7. Click Replicate. The unit restarts in Secondary mode.

15.4.3 Configuring the primary unit

1. From the primary unit login to the AccessIT Manager Web interface.
2. From the **Settings/Maintenance** menu, click **Replication**, Figure 90 appears.
3. Select **Primary Unit**. The page now appears as follows:



This AccessIT unit is a:

○ Standalone Unit

○ Secondary Unit

● Primary Unit

Secondary AccessIT unit IP address: 0 0 0 0

Secondary unit status: Replication is Off

Figure 91 Replication page - Primary Unit

4. Type the IP address of the secondary unit.

5. Click Replicate. The database constantly replicates to the secondary unit.
6. The Secondary Unit status changes to **Replication is on**.

15.4.4 Promoting a secondary unit to a standalone unit

When a primary unit is down or malfunctioning, you can promote the secondary unit to be a standalone unit.

To do so:

1. At the secondary unit login as an Administrator to the AccessIT web interface. See Figure 92.

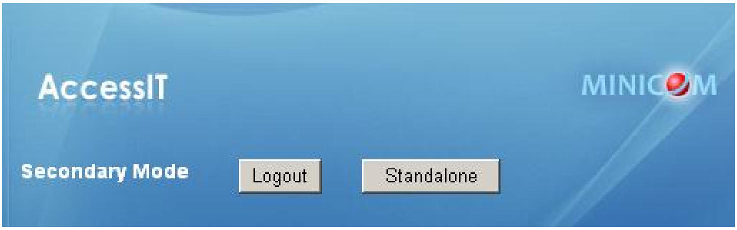


Figure 92 Secondary unit login

2. Press Standalone. The unit restarts in Standalone mode.
3. Re-login to the unit.
4. Change the IP address to match the original primary unit's IP address (The IP address to which all IP devices are pointing). Do this in the **Network** tab under **Settings/Unit Maintenance**, see section 16.2 on page 106. **Note**: Before changing the Secondary unit IP address, switch off or disconnect the original primary unit from the network to avoid network conflicts.
5. Click Save. This unit restarts. Users can login and operate Targets.

15.4.5 Reconfiguring the primary and secondary units

Once the original primary unit has returned, you can set it to be either:

- The primary unit, with the original secondary unit back to its position as secondary unit

Or

- As a secondary unit to the current primary unit

15.4.5.1 Option 1: The original primary unit is the primary unit and original secondary unit is the secondary unit

1. Change the secondary unit status to Standalone mode – see section 15.4.4.
2. At the secondary unit, login to the AccessIT Web interface and backup the database – see section 15.1 on page 94.
3. Change the secondary unit to the secondary unit's IP address.
4. Connect the returned primary unit to the network, power it on and login to the AccessIT Web interface.
5. Restore database on the primary unit machine.
6. Configure the original secondary unit to be the secondary unit and configure the original primary unit to be the primary unit as explained above.

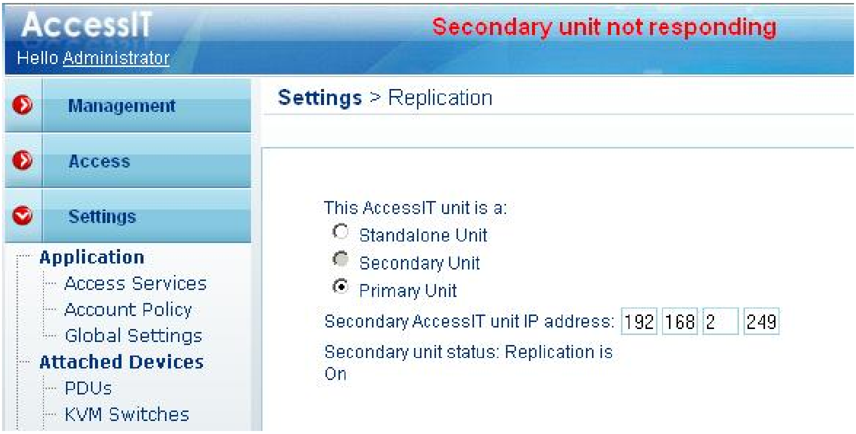
Once completed the continuous database replication starts between primary unit and secondary unit.

15.4.5.2 Option 2. The original secondary unit is the primary unit and the original primary unit is the secondary unit.

1. Before connecting the returned primary unit to the network, switch it on and using a Crossover cable change its IP address to the secondary unit IP address, see section 4.2 on page 18.
2. Connect the returned primary unit to the network.
3. On the returned primary unit login to the AccessIT Manager Web interface and configure it to be the secondary unit as explained above.
4. On the original secondary unit, login to the AccessIT Manager Web interface and configure it to be the primary unit as explained above.

15.4.6 Primary unit and secondary unit troubleshooting

If there is a network failure or the secondary unit is down, a **Secondary unit not responding** notification appears in the AccessIT notification area, indicating that there is a problem connecting to the secondary unit. See figure below.



Secondary unit not responding

This AccessIT unit is a:

○ Standalone Unit

○ Secondary Unit

● Primary Unit

Secondary AccessIT unit IP address: 192 168 2 249

Secondary unit status: Replication is On

Figure 93 System Warning

15.4.7 Checking the secondary unit

1. Verify that the secondary unit is up and running.
2. Verify that the secondary unit is in secondary unit mode.

To do so:

Log in to the secondary unit as an administrator. Check that the unit is in secondary unit mode. If it is not, follow the steps in section 15.4.2 on page 98.

15.4.8 Redoing the secondary and primary unit configuration

Where the secondary unit is verified as up and running and is in secondary unit mode, but the **Secondary unit not responding** or **Secondary unit not replicating** notification persists, do the following:

Convert both the secondary and primary units to standalone mode. To do so:

1. At the primary unit login to the AccessIT web interface. From the **Settings/Maintenance** menu, click **Replication**. Select **Standalone Unit**.
2. At the secondary unit login to the AccessIT web interface and press Standalone. The unit reboots in Standalone mode
3. Convert the secondary unit to secondary unit mode. See section 15.4.2 98
4. Convert the primary unit to primary unit mode. See section 15.4.3 on page 99.

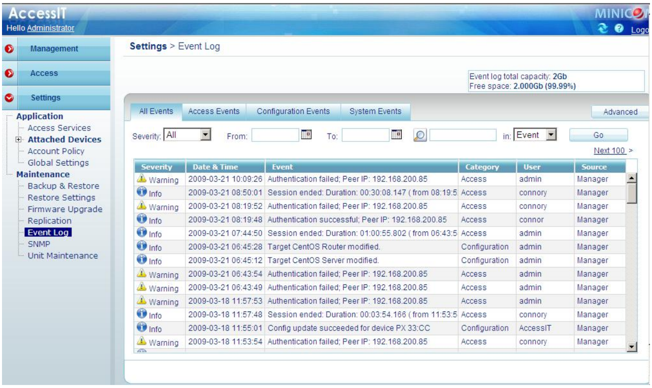
The system should now be operational.

15.5 Event log

You can view an event log of all system activity.

To do so:

1. From the **Settings/Maintenance** menu, click **Event Log**. The Event Log page appears, see Figure 94.



Event log total capacity: **2Gb**
Free space: **2.000Gb (99.99%)**

Severity: All From: To: in: Event

Severity	Date & Time	Event	Category	User	Source
Warning	2009-03-21 10:09:26	Authentication failed; Peer IP: 192.168.200.85	Access	admin	Manager
Info	2009-03-21 08:50:01	Session ended: Duration: 00:30:08.147 (from 08:19:5	Access	connory	Manager
Warning	2009-03-21 08:19:52	Authentication failed; Peer IP: 192.168.200.85	Access	connory	Manager
Info	2009-03-21 08:19:48	Authentication successful; Peer IP: 192.168.200.85	Access	connor	Manager
Info	2009-03-21 07:44:50	Session ended: Duration: 01:00:55.802 (from 06:43:5	Access	admin	Manager
Info	2009-03-21 06:45:28	Target CentOS Router modified.	Configuration	admin	Manager
Info	2009-03-21 06:45:12	Target CentOS Server modified.	Configuration	admin	Manager
Warning	2009-03-21 06:43:54	Authentication failed; Peer IP: 192.168.200.85	Access	admin	Manager
Warning	2009-03-21 06:43:49	Authentication failed; Peer IP: 192.168.200.85	Access	admin	Manager
Warning	2009-03-18 11:57:53	Authentication failed; Peer IP: 192.168.200.85	Access	admin	Manager
Info	2009-03-18 11:57:48	Session ended: Duration: 00:03:54.166 (from 11:53:5	Access	connory	Manager
Info	2009-03-18 11:55:01	Config update succeeded for device PX 33:CC	Configuration	AccessIT	Manager
Warning	2009-03-18 11:53:54	Authentication failed; Peer IP: 192.168.200.85	Access	connory	Manager

Figure 94 Event Log

The columns display the following information:

Severity – activities are recorded as either: Alarm, Warning or Info.

Event – a brief description the event.

Category – type of event either access, system or configuration events.

User – User name that caused the event.

Source – source of the event.

Date & Time – exact date/time of the event.

15.5.1 Drop-down search menus

From the drop-down search menus you can choose the following display options:

Severity – All, Alarm, Warning, Info. Choose to display all events or just a particular category - Alarm, Warning or Info.

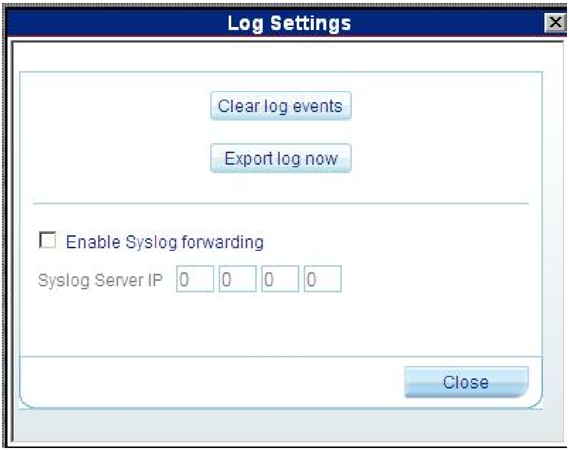
From/To and 🔍 – Search for particular events by selecting a time period in the **From/To** fields. You can fine tune the search by selecting Event, User or Source in the **in:** drop-down menu. Once you select the parameters click Go. The search results appear.

15.5.2 Access, System or Configuration tabs

For convenience, use the **Access**, **System** or **Configuration** tabs to see events in one of these categories only.

15.5.3 Advanced button

Click Advanced, the Log Settings window appears, see Figure 95.



□ Enable Syslog forwarding

Syslog Server IP 0 0 0 0

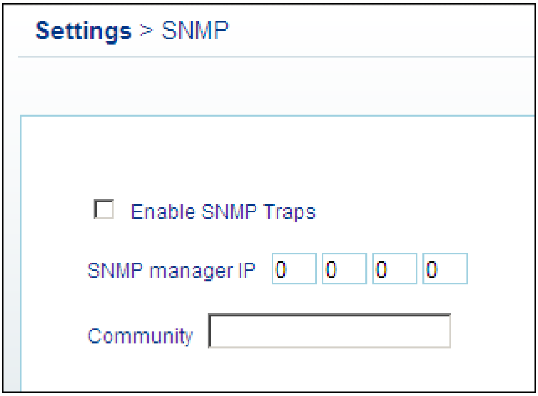
Figure 95 Log Settings window

From here you can clear all log events or export a log to read and/or save as a .csv file. The file can be viewed using Microsoft Excel or compatible software.

15.5.4 Syslog forwarding

To enable Syslog forwarding, select the checkbox in Figure 95 and type the Syslog Server IP address.

15.6 SNMP



Settings > SNMP

□ Enable SNMP Traps

SNMP manager IP 0 0 0 0

Community

Figure 96 SNMP

From this page you can activate or deactivate SNMP logging.

Enable traps - Check to enable sending SNMP traps of AccessIT events and operation.

SNMP Manager IP - Enter the SNMP Server IP address.

Community – type the SNMP community.

16. Unit Maintenance

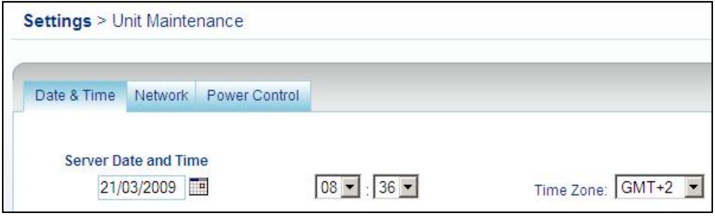
From the **Settings/Maintenance** menu, click **Unit Maintenance**, Figure 97 appears.

Here you set:

- Server date and time
- Network parameters
- Power control

16.1 Date & Time tab

Set the server date and time and choose the time zone. These parameters are used in the Event log, in scheduled backups and in CFG updates.

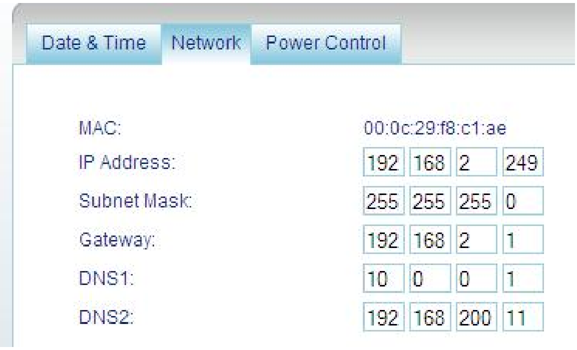


Server Date and Time
21/03/2009 08 : 36 Time Zone: GMT+2

Figure 97 Unit Maintenance

16.2 Network tab

Click the **Network** tab, the following appears.



MAC: 00:0c:29:f8:c1:ae
IP Address: 192 168 2 249
Subnet Mask: 255 255 255 0
Gateway: 192 168 2 1
DNS1: 10 0 0 1
DNS2: 192 168 200 11

Figure 98 Network tab

Here you can change the network parameters of the AccessIT unit. The unit restarts after changing the IP settings.

Important! For computer name resolving and operation in LDAP mode, DNS servers must be set in the Network tab.

16.3 Power Control tab

Click the **Power Control** tab, the following appears.

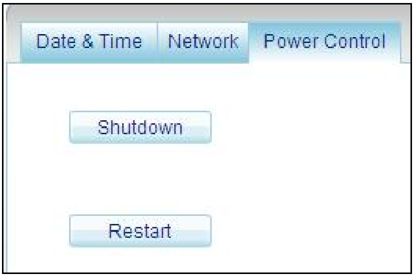


Figure 99 Power Control tab

For maintenance purposes:

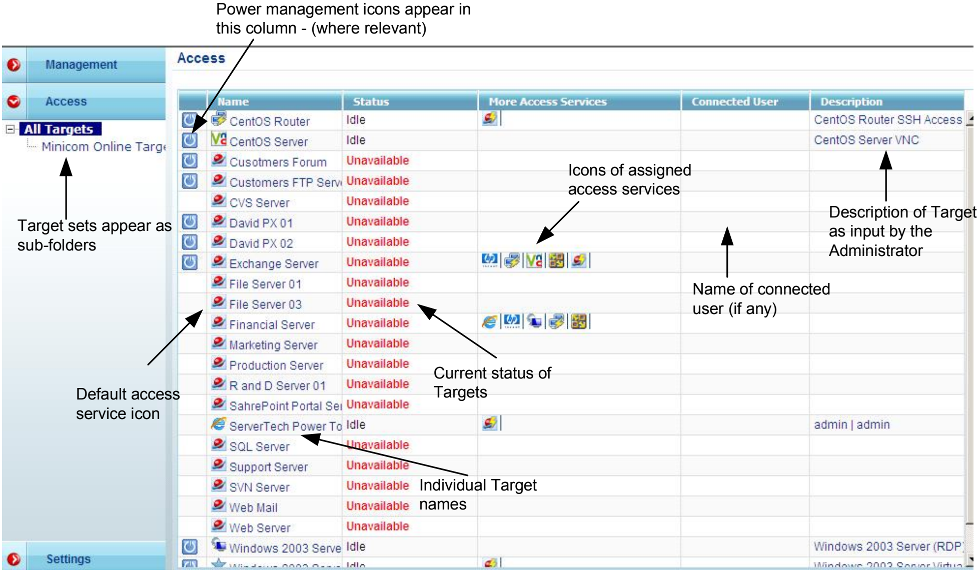
To shutdown the AccessIT unit click Shutdown.

To restart the AccessIT unit click Restart.

17. Accessing Targets - Administrator

For an Administrator to access a Target:

From the menu, select **Access**. The Access page appears showing the individual Targets the Administrator is currently allowed to access. See Figure 100.



Power management icons appear in this column - (where relevant)

Access

	Name	Status	More Access Services	Connected User	Description
⏻	CentOS Router	Idle			CentOS Router SSH Access
⏻	CentOS Server	Idle			CentOS Server VNC
⏻	Cusotmers Forum	Unavailable			
⏻	Customers FTP Serv	Unavailable			
	CVS Server	Unavailable			
⏻	David PX 01	Unavailable			
⏻	David PX 02	Unavailable			
⏻	Exchange Server	Unavailable			
	File Server 01	Unavailable			
	File Server 03	Unavailable			
	Financial Server	Unavailable			
	Marketing Server	Unavailable			
	Production Server	Unavailable			
	R and D Server 01	Unavailable			
	SahrePoint Portal Sei	Unavailable			
	ServerTech Power To	Idle			admin | admin
	SQL Server	Unavailable			
	Support Server	Unavailable			
	SVN Server	Unavailable			
	Web Mail	Unavailable			
	Web Server	Unavailable			
⏻	Windows 2003 Serve	Idle			Windows 2003 Server (RDP)

Target sets appear as sub-folders

Default access service icon

Icons of assigned access services

Current status of Targets

Individual Target names

Name of connected user (if any)

Description of Target as input by the Administrator

Figure 100 Access page

17.1 Access page columns

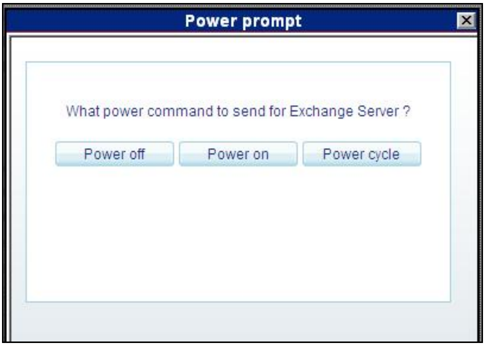
The Access page columns contain the following:

17.1.1 Power management column

When there are power management devices (PDUs) connected to the Targets / KVM switches, a Power icon ⏻ appears in this column, from which you can power manage the Target.

To power manage a Target:

1. Click ⏻. The Power prompt appears, see Figure 101.
2. Click the relevant button to power off/on or power cycle.



Power prompt

What power command to send for Exchange Server ?

Figure 101 Power prompt

17.1.2 Name column

This column includes the name of the Target and the default Access Service icon. This icon represents the Access Service that is used by default to access the Target when the Target name (or Access Service icon) is clicked. To use a different Access Service, click it in the More Access Services column.

17.1.3 Status column

The **Status** column gives the current status of the Target as follows:

Available –A user can press the Target name link and establish a remote session to that Target.

Remote Active Session – A user is currently connected.

Unassigned – The Target is not assigned to any IP device.

Updating device – Device is receiving an updated configuration from AccessIT Manager, and cannot currently serve remote sessions.

Unavailable – IP device is not available (IP device is itself in **Alarm** status).

Busy – This refers to a server connected to an IP device via a KVM switch. A user or users are currently accessing other servers connected to that KVM switch and no more servers can be accessed.

Local active session – (Only appears for the DX matrix and some other matrix switches). A local user is currently connected.

Idle – All Targets assigned to non KVM/IP access services display Idle in the Status column.

17.1.4 More access services column

All configured Access Services appear here. The default service always appears next to the Target name. To use a different Access Service, click it in the More

Access Services column. When you hold the mouse over an icon, a tooltip appears with the name of the Access Service.

Note! For connecting to Serial Console Targets, you must click the icon in the More Access Services column.

17.2 Accessing a Target via KVM/IP remote session

1. Click a Target or Minicom Globe icon . The Remote console window with the Target's screen and toolbar appear, see Figure 102.

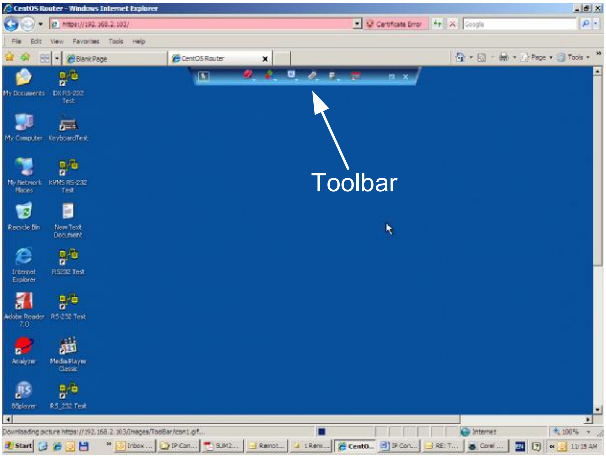


Figure 102 Remote console window

On the remote console you have the following:

Target name - The currently accessed server identity can be checked by looking at the Server name on the Internet Explorer title bar.

17.3 Sharing a remote session

When connecting to a Target Server that other users are already connected to, the following message appears.

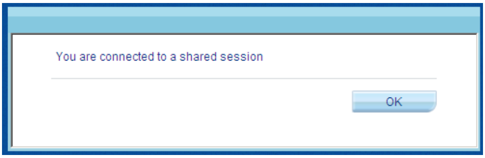

You are connected to a shared session

Figure 103 Busy remote session

Up to 5 users can share the same remote session.

17.3.1 Private remote session

When starting a remote session and there are no other logged in users a user can prevent other users from connecting to his session, from the Toolbar – see **Exclusive session** on page 113.

17.4 Displaying the Toolbar

The Toolbar appears briefly at the top of the screen, see Figure 102. It disappears when the mouse is not over it. To make it reappear, glide the mouse over the top of the screen. To display the Toolbar permanantly, click the tack icon on the Toolbar.

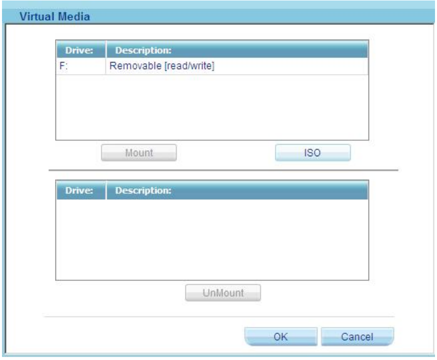
17.5 Virtual Media

Virtual Media – (only appears when the Target is connected to a PX USB). With Virtual Media you can mount virtually onto the Target, removable mass storage devices connected to the Client computer.

This includes:

- Floppy drive
- CD-ROM
- DVD-ROM
- ISO Image of CD\DVD
- USB Flash Drives (Disk on key tokens)
- Miscellaneous USB memory sticks/cards identified by the operating system as removable mass storage devices

1. From the Toolbar click /Virtual Media, the Virtual Media dialog box appears, see Figure 104.



Virtual Media

Drive:	Description:
F:	Removable [read/write]

Drive:	Description:

Figure 104 Virtual Media

All connected mass storage devices appear in the **Local Drives** section.

2. Select the device to be mounted and click **Mount**. The device mounts onto the Target and appears as a removable or CD/DVD drive of the Target. It also appears in the **Mounted Drives** section in Figure 104. Once mounted, you can use the device during the remote session as if it is connected to the Target.

Mounting an ISO file

An ISO image (.iso) is a disk image of an ISO 9660 file system, and refers to any optical disc image, even a UDF image. In addition to the data files in the ISO image, it also contains all the file system metadata, including boot code, structures, and attributes. All of this information is contained in a single file. These properties make it an attractive alternative to physical media for the distribution of software that requires this additional information as it is simple to retrieve over the Internet.

To mount an ISO file, click **Mount ISO File**, locate the file and mount it.

17.5.1 Things to know during operation of the Virtual Media

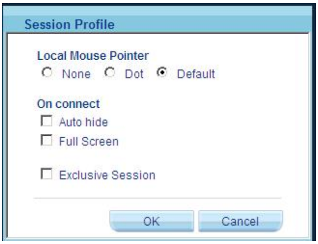
Because Virtual Media emulates USB 1.1 over a TCP connection it has a number of limitations which govern the Virtual Media compatibility and operation.

- Virtual Media emulates USB 1.1. It doesn’t emulate USB 2.0
- Virtual Media redirects the Clients local DVD/CD or removable mass storage devices to a Target computer during the open client session only. This means if the remote client session disconnects, the mounted drives will be automatically dismounted in the Target computer.
- Maximum data transfer speed of the Virtual Media doesn’t exceed 5.0 Mb/s
- Only drives identified by the Client Operating System as Drives with Removable Storage can be mounted as a Virtual Media. Many USB attached hard disks identify themselves to the Operating System as Hard Disk Drives and can’t be used for Virtual Media mounting.
- Booting from mounted virtual media drive is possible only if the Target computer supports boot from USB attached storage.
- Currently, it is not possible to boot a Target computer from Linux distribution mounted as a Virtual Media.
- Windows CD/DVD or its modifications as Winternals ERD Commander, WinPE, BartPE, or similar can be used for booting the Target computer when mounted as a Virtual Media.

- Mounting Removable mass storage devices as USB Flash Drives (Disk on key tokens) or miscellaneous USB memory sticks/cards will remove them from Client Operating System and redirect with Read/Write access permissions to the Target computer to ensure integrity of Write operation.
- Connection timeout will not occur all the time the Virtual Media is remained mounted.
- PX USB with firmware version 3.0.2.27 or higher has Virtual Media capabilities. Older versions of PX USB may not have this capability or may have a limited set of features.

17.6 Session profile

You have several remote session display options to choose from. From the Toolbar click / Session Profile. The Session Profile box appears, see Figure 105.



Session Profile

Local Mouse Pointer
○ None ○ Dot ● Default

On connect
□ Auto hide
□ Full Screen

□ Exclusive Session

Figure 105 Session Profile box

You have the following options:

Local Mouse Pointer – You can change the Client computer mouse pointer to appear as a dot or to not appear at all. Default is a regular shaped mouse cursor.

On connect

Auto Hide – Check this option to hide the Toolbar from the next connection onwards.

Full Screen - Check this option to make the remote session screen appear in full screen mode from the next connection onwards. To toggle the full screen mode on and off, press **F11**. (See section 17.7 below).

Exclusive Session - When starting a remote session and there are no other logged in users, a user can prevent other users from logging into the session by selecting the Exclusive Session checkbox.

17.7 Full screen mode

Work on the Target Server as if you are working on a local computer, with full screen mode.

To work in full screen mode:

1. Ensure that the Client computer has the same screen resolution as the Target Server.
2. Press **F11**. The browser window disappears.

To exit full screen mode:

Press **F11**. Or place the mouse at the top of the window to display the browser toolbar and click the Restore button .

Note! Full screen mode can also be activated from the Session Profile box, see above.

About

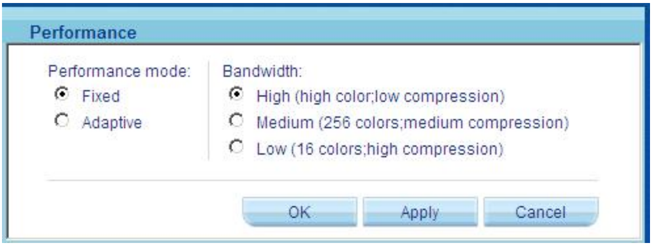
Click /About to verify the Client, Firmware, KME (Keyboard/Mouse Emulation firmware) and Switch file versions installed on your IP device.

17.8 Changing the performance settings

You can alter the performance settings from the Toolbar.

To alter the settings:

From the Toolbar, click /Performance. The Performance dialog box appears, see Figure 106.



Performance

Performance mode:
● Fixed
○ Adaptive

Bandwidth:
● High (high color;low compression)
○ Medium (256 colors;medium compression)
○ Low (16 colors;high compression)

Figure 106 Performance box

Performance mode

You can choose fixed or adaptive – these are explained below.

Fixed mode

Fixed mode allows you to select the high, medium or low bandwidth option. For example, in a LAN environment, it is best to set the bandwidth setting on High. For VPN and internet environments you may want to alter the settings to increase responsiveness.

Bandwidth - Choose from the following options

High - For optimal performance when working on a LAN, select High. This gives a low compression and high colors (16bit).

Medium - Select medium for medium compression and 256 colors. Medium is recommended when using a standard internet connection.

Low - Select Low for high compression and 16 colors.

Adaptive mode

Adaptive mode automatically adapts to the best compression and colors according to the network conditions.

Click **OK**. The chosen setting take effect and the screen of the last accessed Target Server appears.

17.9 Adjusting the Video settings

To change the video settings:

From the Toolbar, click . You have the following options:

- Refresh
- Video Adjust
- Advanced

Each option is explained below.

17.9.1 Refresh

Select Refresh to refresh the Video image. Refresh may be needed when changing the display attributes of a Target Server.

17.9.2 Video Adjust

To adjust the video automatically:

Click **Video Adjust**. The process takes a few seconds. If the process runs for more than 3 times, there is an abnormal noise level. Check the video cable and verify that no dynamic video application is running on the Target Server’s desktop.

Perform the procedure where necessary for each Target Server or new screen resolution.

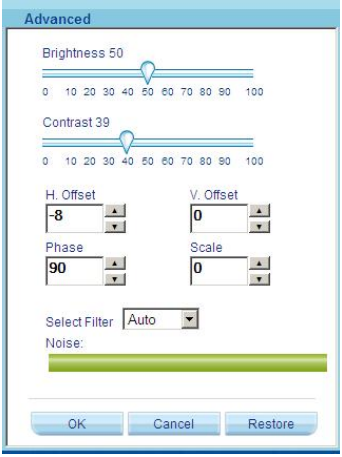
17.9.3 Advanced

Use the Advanced video adjustment options for fine-tuning the Target Server video settings after auto adjustment or for adapting to a noisy environment or a non-standard VGA signal or when in full-screen DOS/CLI mode.

To adjust the video:

Click Advanced. The manual controls appear, see Figure 107.

After adjusting the video manually, you can always revert to Auto settings by clicking Auto Video Adjust – explained in section 17.9.2 below.



Advanced

Brightness 50

Contrast 39

H. Offset: -8

V. Offset: 0

Phase: 90

Scale: 0

Select Filter: Auto

Noise:

Figure 107 Manual Video Adjustments controls

Brightness / Contrast - use the scales to adjust the brightness and contrast of the displayed image. Move the sliders to change the displayed image. Click in the area of the sliders for fine-tuning.

For the following controls choose the appropriate measurement.

H. Offset - defines the starting position of each line on the displayed image.

V. Offset - defines the vertical starting position of the displayed image.

Phase - defines the point at which each pixel is sampled.

Scale – defines the scale resolution of the session image.

Adjust Phase and Scale to reduce noise level to a minimum.

Select Filter - defines the filter of the input video from the server. A higher filter reduces the noise level but makes the image heavier.

Noise - represents the Video "noise" when a static screen is displayed.

17.10 Power cycle

Where a Minicom Remote Power switch or POC is connected to the Serial port of the IP device, you can power manage the Target servers as follows:

From the Toolbar, click ⏻. The Power menu appears, see below.

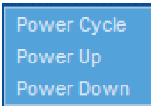


Figure 108 Power menu

To send a power cycle command or to power down or up the currently accessed Target server, select the appropriate option.

Note! Only the currently accessed Target server is affected, so to power manage other Target servers you must access each one individually.

17.11 Keyboard key sequences

Click ⌨. A list of defined keyboard sequences appears. When clicked, these transmit directly to the Target Server, and will not affect the Client computer.

For example, select **Ctrl-Alt-Del** to send this three key sequence to the Target Server to initiate its Shutdown/Login process.

To add a keyboard sequence:

Click **Add/Remove**. The Special Key Manager box appears see Figure 109.

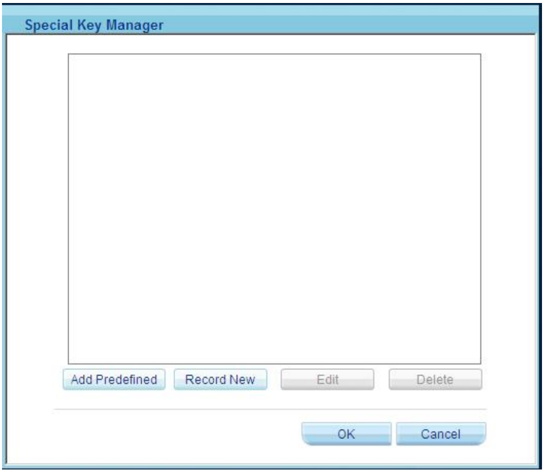


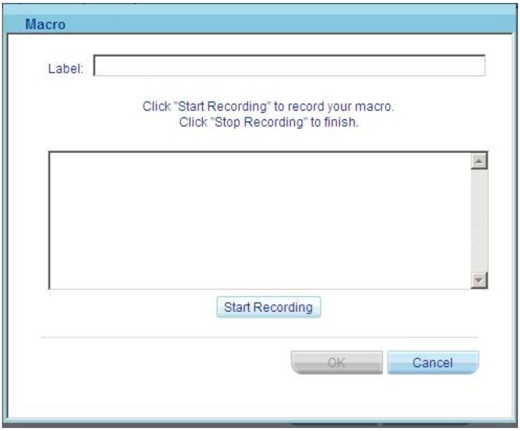
Figure 109 Special Key Manager box

To add a predefined sequence:

1. Click Add Predefined. A list of sequences appears.
2. Select the desired sequence and click OK. The sequence appears in the Special Key Manager box.
3. Click OK. The sequence appears in the Keyboard Key sequence list.

To record a key sequence:

1. From the Special Key Manager box press **Record New**. The Macro box appears see Figure 110.



Macro

Label:

Click "Start Recording" to record your macro.
Click "Stop Recording" to finish.

Figure 110 Macro box

2. Give the key sequence a name in the Label field.
3. Click **Start Recording**.
4. Press the desired keys. The keys appear in the area provided.
5. Click **Stop Recording**.
6. Click **OK**.

To edit a key sequence:

1. From the Special Key Manager box select the desired key.
2. Click **Edit**.
3. Click **Start Recording**
4. Press the desired keys. The keys appear in the area provided.
5. Click **Stop Recording**.
6. Click **OK**.

17.12 Synchronizing mouse pointers

When working at the Client computer, two mouse pointers appear: The Client computer's is on top of the Target Server's. The mouse pointers should be synchronized. The following explains what to do if they are not synchronized.

> **Warning**
>
> Before synchronizing mouse pointers adjust the video of the Target Server, (explained above) otherwise mouse synchronization may not work..

17.12.1 Aligning the mice pointers

When accessing the Target Server, the mice may appear at a distance to each other.

To align the mouse pointers:

From the Toolbar click 🖱 / **Align**. The mice align.

17.12.2 Calibrating mice pointers

A Target Server may have a different mouse pointer speed to the Client computer. Calibrating automatically discovers the mouse speed of the Target Server and aligns the two pointers.

To perform the calibration when the Target Server Operating system is, Windows NT4, 2000 or 98:

From the Toolbar click 🖱 / **Calibrate**. The IP device saves this alignment so calibration is only needed once per Target Server.

If the Video Noise Level is above zero, calibration may not work. Go to Video Adjustment and try to eliminate the noise by pressing Auto video adjust and/or adjusting the bars in Manual video adjust, then perform the mouse calibration.

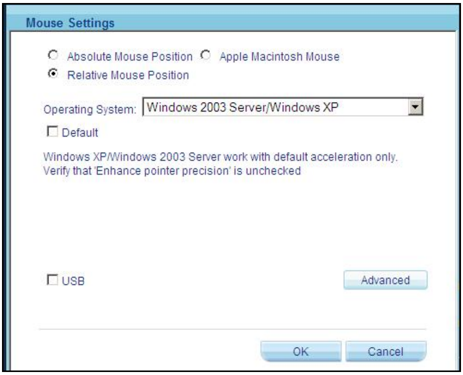
Note! If the mouse settings on the Target Server were ever changed, you must synchronize mouse pointers manually, as explained below.

17.13 Manual mouse synchronization

If the mouse settings on the Target Server were ever changed, or when the Operating system on the Target Server is, Windows XP or later, Linux, Novell, SCO UNIX or SUN Solaris you must synchronize the mouse pointers manually.

To manually synchronize mouse pointers:

1. From the Toolbar click 🖱 / **Mouse Settings**. The **Mouse Settings** box appears see Figure 111.



Mouse Settings

○ Absolute Mouse Position ○ Apple Macintosh Mouse
● Relative Mouse Position

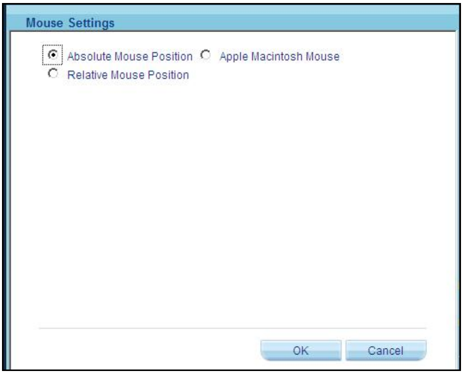
Operating System: Windows 2003 Server/Windows XP

□ Default

Windows XP/Windows 2003 Server work with default acceleration only.
Verify that 'Enhance pointer precision' is unchecked

□ USB

Figure 111 Relative Mouse Settings



Mouse Settings

● Absolute Mouse Position ○ Apple Macintosh Mouse
○ Relative Mouse Position

Figure 112 Absolute Mouse Settings

17.13.1 Relative/Absolute Mouse Position/Apple Macintosh

Absolute Mouse Position and Apple Macintosh are only relevant for PX USB KVM/IP devices (see section 17.13.2 below). All other KVM/IP devices must have Relative Mouse Position selected - which is the default.

17.13.1.1 Relative Mouse Position

1. From the drop down menu, select the Target's Operating system. Instructions and sliders appear.
2. Follow the instructions and set any relevant sliders to the same values as set in the Target's Mouse Properties window.
3. Click **OK** to save the settings.

2 examples!

For Windows XP. Go to the Mouse settings on the Target and uncheck Enhance pointer precision.

For Windows 2000. If Mouse Properties were ever changed for the Target – even if they have been returned to their original state - uncheck default ☑ Default.

Click **OK**. The mouse pointers should be synchronized.

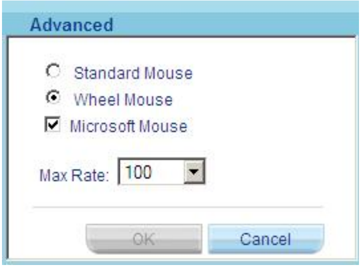
17.13.1.2 USB

The **USB** option in the Mouse Settings box is available for USB to PS/2 adapters, RICC/ROC USB, X-RICC USB and Phantom Specter USB and for unsupported operating systems and SUN Solaris. Use this option if you are sure of the custom acceleration algorithm you are using, or have been informed so by customer support.

17.13.1.3 Advanced – Mouse Emulation

In the Advanced Mouse settings, you can set the type of mouse that you would like the IP device to emulate. We recommend not changing the advanced settings unless there is erratic mouse behavior (the mouse is making random clicks and jumping arbitrarily around the screen).

Click Advanced the Mouse Emulation box appears see Figure 113.



○ Standard Mouse
● Wheel Mouse
☑ Microsoft Mouse

Max Rate: 100

Figure 113 Mouse Emulation box

Select the mouse connected to the Local Console port on the IP device, e.g. if the local mouse is a non-Microsoft 2 button mouse, select **Standard Mouse** and uncheck **Microsoft Mouse**.

Max Rate - this defines the maximum mouse report rate. For Sun Solaris the default value is 20 in order to support older Sun versions.

17.13.2 PX USB KVM/IP

For PX USB KVM/IP devices:

- If the Operating system on the Target is, Windows ME or later, select Absolute Mouse mode, see Figure 112.
- If the Operating system on the Target is, Windows 98 or Linux, Novell, UNIX or SUN, select Relative Mode.
- If the Target is a MAC computer, select Apple Macintosh.

17.13.3 Switching to a different server

There are 2 methods of switching to a different server.

(A) Select a different Target from the AccessIT Access page.

(B) Where the Target you wish to switch to is connected to the same IP device as the current Target:

1. From the Toolbar, click . A list of available servers appears. The currently connected server is highlighted in bold.
2. Click the desired server name. The screen of the selected server appears.

<u>For DXU IP II - In enabled and Managed modes</u>, - First login to the AccessIT and then select the server you want to access on the Access page. If the system is working in enabled mode, the AIM login will appear. Login to the AIM and then select the required server from the IP toolbar again. Switch between the servers using the IP toolbar or AccessIT Manager.

<u>Important!</u> Accessing or switching to the servers from the IP toolbar, only works when the DX AIM is on the Servers/Devices page.

17.13.4 Disconnecting the remote session

To disconnect the session, on the Toolbar, click ×. The Login page appears. You can re-login or close the browser window.

For DXU IP II - For **<u>managed</u>** mode the User disconnects from the server and from the remote session.

For **<u>enabled</u>** mode the User disconnects from the server and from the remote session. The DXU IP II remains logged into the AIM.

17.14 Accessing a Target through other Access Services

Default Access Service

Where the Access Service is the default Access Service, its icon appears in the **Name** column on the **Access** page.

To access the Target:

Click the icon or the Target name on the **Access** page.

Not default Access Service

Where the Access Service is not the default Access Service, its icon appears in the **More Access Services** column on the **Access** page.

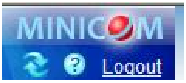
To access the Target:

Click the icon in the **More** Access **Services** column on the **Access** page.

Access to the Target works according to the type of service accessed and according to the parameters as configured in section 10.3 on page 55.

17.15 Exiting the AccessIT system

To exit the system:

Just below the Minicom logo 

, click **Logout**. The login screen appears and you are logged out.

Note: Exiting the AccessIT Manager has no effect on open user sessions

18. Accessing Targets as a User

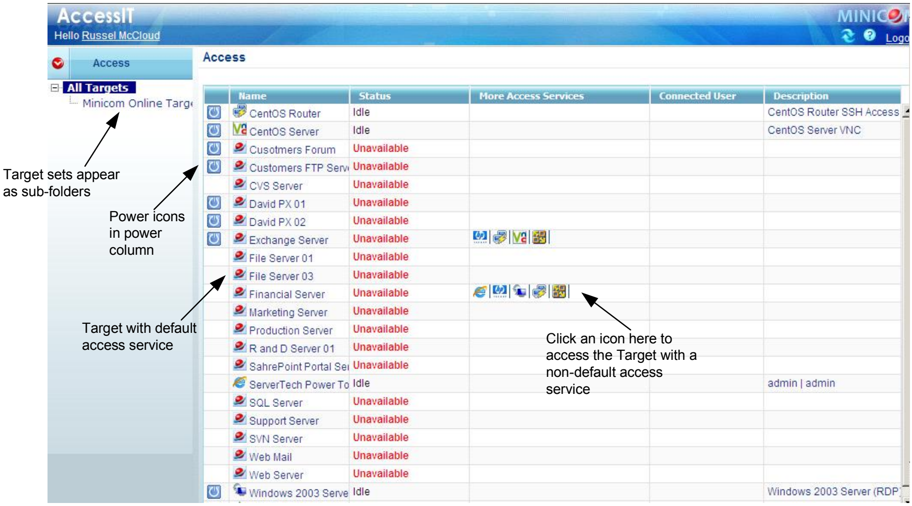
Once the Administrator has set up and configured the AccessIT system, Users can access the system and connect to permitted Targets.

For a User to access the system:

Type the AccessIT Manager IP address (https://*IP address*) into a Web browser and press **Enter**. The Login page appears.

Type the Username and Password and press **Enter**. The **Access** page appears see Figure 114. The window displays only Targets and Target Sets that the User has permission to access.

Note! AccessIT system supports multi-user login. There is no limit to the amount of concurrent users.


AccessIT
Hello Russel McCloud
MINICO
Logo
Access
All Targets
Minicom Online Targ
Target sets appear as sub-folders
Power icons in power column
Target with default access service
Click an icon here to access the Target with a non-default access service

Access

	Name	Status	More Access Services	Connected User	Description
⏻	CentOS Router	Idle			CentOS Router SSH Access
⏻	CentOS Server	Idle			CentOS Server VNC
⏻	Cusotmers Forum	Unavailable			
⏻	Customers FTP Serv	Unavailable			
	CVS Server	Unavailable			
⏻	David PX 01	Unavailable			
⏻	David PX 02	Unavailable			
⏻	Exchange Server	Unavailable			
	File Server 01	Unavailable			
	File Server 03	Unavailable			
	Financial Server	Unavailable			
	Marketing Server	Unavailable			
	Production Server	Unavailable			
	R and D Server 01	Unavailable			
	SahrePoint Portal Se	Unavailable			
	ServerTech Power To	Idle			admin | admin
	SQL Server	Unavailable			
	Support Server	Unavailable			
	SVN Server	Unavailable			
	Web Mail	Unavailable			
	Web Server	Unavailable			
⏻	Windows 2003 Serve	Idle			Windows 2003 Server (RDP

Figure 114 User Access page

18.1 Power column

When there are power management devices (PDUs) connected to the targets / KVM switches, a Power icon appears in this column, from which you can power manage the Target. The operation is the same as that for an administrator, see section 17.1.1 on page 108.

18.2 Status column

The Status column gives the User the current status of the Target as follows:

Available – The user can click the Target name or Access Service icon and establish the remote session to that Target.

Remote Active Session – A user is currently connected.

Unassigned – The Target is not assigned to any IP device.

Updating device – Device is receiving an updated configuration from AccessIT Manager, and cannot currently serve remote sessions.

Unavailable – IP device is not available (IP device is itself in **Alarm** status).

Busy – This refers to a server connected to an IP device via a KVM switch. A user or users are currently accessing other servers connected to that KVM switch and no more servers can be accessed.

Local active session – (Appears only for the DX matrix). A local user is currently connected.

Idle – All Targets assigned to non KVM/IP access services display Idle in the Status column.

18.3 Connecting to a Target

The **Access** page displays all Targets that the user has permission to access. Target Sets appear as sub-folders. Click a **Target Set** to display the Targets in that Set.

18.3.1 Connecting to a KVM/IP device Target

To connect to a KVM/IP device Target:

Click the Target name. The Target's screen appears. To connect using a non-default access service, click the desired icon in the **More Access Services** column. Hold the mouse over an icon to display a tooltip of the Access Service name.

18.3.2 Connecting to a non-KVM/IP device Target

To connect to a non-KVM/IP device Target:

Default Access Service

Where the non-KVM/IP Access Service is the default Access Service, its icon appears in the **Name** column on the **Access** page.

To access the Target:

Click the icon or the Target name on the **Access** page.

Not default Access Service

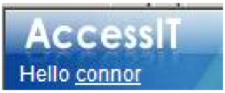
Where the non-KVM/IP Access Service is not the default Access Service, its icon appears in the **More Access Services** column on the **Access** page.

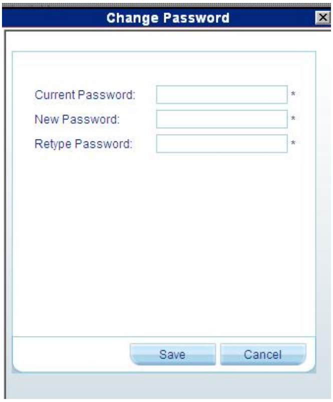
To access the Target:

Click the icon in the **More Access Services** column on the **Access** page.

Access to the Target works according to the type of service accessed and according to the parameters as configured in section 10.3 on page 55. There is no difference connecting to KVM/IP or to any other Access Service (VNC, RDP etc.).

18.3.3 Changing the password

Click the user name below AccessIT . The **Change Password** window appears, see Figure 115.



Change Password

Current Password: *

New Password: *

Retype Password: *

Figure 115 Change Password window

Type and retype a new password, then press **Save**. The new password is saved.

An Administrator can change his password in the same way.

19. Accessing an IP device directly

If the AccessIT system is down e.g. for maintenance, the availability of each IP device remains. You can access an IP device unit directly by entering its IP address into your web browser.

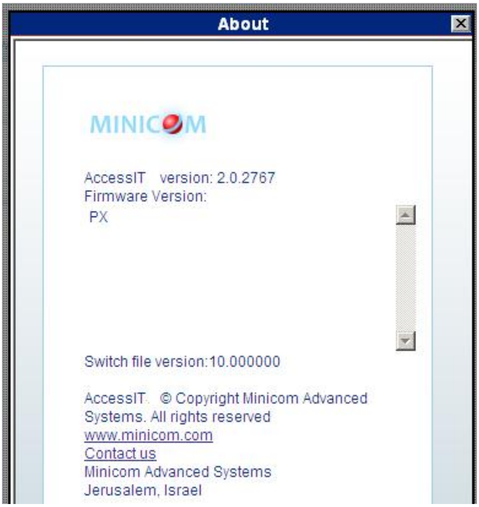
Note! This is only if the system is working in Local Authentication mode and not in External Authentication (LDAP) mode.

To change any hardware elements and user authorization from the IP device, you must first uncheck Enable Centralized Management in the IP device Network Configuration window.

20. About

Click AccessIT at the top of the page, the **About** page appears, see Figure 116. This contains information about the version of the:

- AccessIT firmware
- IP devices firmware
- Switch definition file



AccessIT version: 2.0.2767
Firmware Version:
PX

Switch file version:10.000000

AccessIT © Copyright Minicom Advanced Systems. All rights reserved
www.minicom.com
Contact us
Minicom Advanced Systems
Jerusalem, Israel

Figure 116 About page

21. General troubleshooting

A) An IP device is not responding

1. Confirm that the unit is powered on and its network cable is connected properly.
2. Confirm the IP settings are correct and you can route to the unit.
3. Confirm that the IP device in not in the middle of an upgrade process.
4. Restore the device to factory defaults and reconfigure it.

B) An IP device displays an Alarm status

1. Confirm that the IP device is in working order.
2. Confirm the device IP settings.
3. Delete and reconfigure the IP device on the AccessIT.

C) When clicking on a Target I get an error 900.. cannot connect

1. Try to restart the unit and wait until it's online.
2. Ensure that port 900 is not blocked by another application.
3. Ensure there are no duplicated IP devices on the network with the same settings.
4. Verify the device has a firmware version compatible with AccessIT.

D) When controlling a Target the mouse cannot be synchronized

1. Make sure that the Operating System selection and the Mouse Acceleration / Threshold settings on the AccessIT Target properties match the server parameters.
2. If using a KVM Switch with USB dongle or USB to PS/2 adaptor, ensure that the 'USB Converter' checkbox is checked in the AccessIT Target properties.
3. Try to disable mouse acceleration on the Target and to select 'None' in the Acceleration field in the AccessIT Target properties.

E) The Video is distorted when controlling a Target

1. Push the ‘Auto Video Adjust’ button in the Client video settings.
2. Confirm that this particular IP device can show clear video on an already confirmed server.
3. Replace the 3-in-1 cable or test it on another KVM switch.
4. Try changing the Target screen resolution or refresh rate.

F) Performance decreases when controlling a Target

1. Click the ‘Auto Video Adjust’ button in the Client video settings.
2. Reduce the colors or compression levels in the Client Performance settings.
3. Check that video from the Target is clear with low noise level.

G) Legacy KVM port switching does not occur

1. Check the cable connectivity from the KVM/IP device to the KVM Switch.
2. Confirm that from the local console (using the KVM Switch hotkey) you can switch between the KVM ports.
3. Confirm that the KVM Switch selection on the AccessIT matches the KVM Switch hotkey definition.

H) Cannot login to the AccessIT

1. If the AccessIT is configured to work with LDAP server (Windows 2003 Server Active Directory) authentication, ensure that connection between the AccessIT and Active Directory is working properly.
2. Restore the unit to factory default settings. Login with the admin/access account and then restore the AccessIT database backup.

J) All devices display Alarm mode after a firmware upgrade of the AccessIT Manager

Repeat the upgrade. The AccessIT Manager restarts automatically after the upgrade. The AccessIT had not completed the restart process.

K) I am unable to see the AccessIT web interface without error messages appearing

For added security, a Safenet Sentinel Security key is connected internally to a USB port of AccessIT Manager.

If the key is disconnected during operation of the system, Users are unable to login, and error message appears.

Users that were logged in before the key was disconnected are unaffected by the key being disconnected.

To allow access, reconnect the Safenet Sentinel Security key and restart the AccessIT Manager.

22. Technical Specifications

Operating systems	**Target Server** DOS, Windows, Novell, Linux, SUN Solaris for PC **Client Computer** Windows 2000 and later with Internet Explorer 6 and later or Firefox 3 and later Linux x86 and Firefox 3 and later
Authentication	Local or Microsoft Active Directory
Security	SSL, high grade 256-bit AES encryption
Maximum # of users	20
Maximum # of IP devices	50
Maximum # of targets	250 (servers and network devices)
Replication unit	Yes
Backup / Restore	Yes
Device configuration	Automatic discovery of Minicom IP KVM devices
Firmware upgrade	Yes
Protocols	HTTPS, XML, SSH, Telnet, LDAP
Form factor	1U x 19” rack mountable
Network connection	RJ45
Power supply	115-230 VAC, 50-60Hz autosensing

Environmental	
Temperature	Operating 10° to 35°C (50° to 95°F) Storage –40° to 65°C (–40° to 149°F)
Relative humidity	Operating 20% to 80% (non-condensing) with a maximum humidity gradation of 10% per hour Storage 5% to 95% (non-condensing)
Maximum vibration	Operating 0.26 Grms at 5–350 Hz for 15 min Storage 1.54 Grms at 10–250 Hz for 15 min
Maximum shock	Operating One shock pulse in the positive z axis (one pulse on each side of the system) of 31 G for up to 2.6 ms Storage Six consecutively executed shock pulses in the positive and negative x, y, and z axes (one pulse on each side of the system) of 71 G for up to 2 ms
Altitude	Operating –16 to 3,048 m (–50 to 10,000 ft) NOTE: For altitudes above 2,950 feet, the maximum operating temperature is derated 1°F/550 ft. Storage –16 to 10,600 m (–50 to 35,000 ft)
Airborne contaminant level	Class G2 or lower as defined by ISA-S71.04-1985

22.1 WEEE compliance

WEEE Information for Minicom Customers and Recyclers

Under the Waste Electrical and Electronic Equipment (WEEE) Directive and implementing regulations, when customers buy new electrical and electronic equipment from Minicom they are entitled to:

- Send old equipment for recycling on a one-for-one, like-for-like basis (this varies depending on the country)
- Send the new equipment back for recycling when this ultimately becomes waste

Instructions to both customers and recyclers/treatment facilities wishing to obtain disassembly information are provided in our website www.minicom.com.

23. Appendix A – PX details

PX

Identifying Name - e.g.
by location

____

MAC address

____

Target server

Identifying Name

____

OS _____________

Mouse settings *:
Acceleration______
Threshold________

PX

Identifying Name - e.g.
by location

____

MAC address

____

Target server

Identifying Name

____

OS _____________

Mouse settings *:
Acceleration______
Threshold________

PX

Identifying Name - e.g.
by location

____

MAC address

____

Target server

Identifying Name

____

OS _____________

Mouse settings *:
Acceleration______
Threshold________

PX

Identifying Name - e.g.
by location

____

MAC address

____

Target server

Identifying Name

____

OS _____________

Mouse settings *:
Acceleration______
Threshold________

PX

Identifying Name - e.g.
by location

____

MAC address

____

Target server

Identifying Name

____

OS _____________

Mouse settings *:
Acceleration______
Threshold________

PX

Identifying Name - e.g.
by location

____

MAC address

____

Target server

Identifying Name

____

OS _____________

Mouse settings *:
Acceleration______
Threshold________

PX

Identifying Name - e.g.
by location

____

MAC address

____

Target server

Identifying Name

____

OS _____________

Mouse settings *:
Acceleration______
Threshold________

PX

Identifying Name - e.g.
by location

____

MAC address

____

Target server

Identifying Name

____

OS _____________

Mouse settings *:
Acceleration______
Threshold________

*** Only needed when not default**

23.1 KVM/IP device details

IP device

Identifying Name - e.g.
by location

____

MAC address

____

KVM switch
(where relevant)

Switch type

____

Number of ports

____

Local mouse type -
Standard 2 button / Wheel

Target server

Identifying Name

____
Port number_______
OS _____________

Mouse settings *:
Acceleration______
Threshold_______

Target server

Identifying Name

____
Port number_______
OS _____________

Mouse settings *:
Acceleration______
Threshold_______

Target server

Identifying Name

____
Port number_______
OS _____________

Mouse settings *:
Acceleration______
Threshold_______

Target server

Identifying Name

____
Port number_______
OS _____________

Mouse settings *:
Acceleration______
Threshold_______

Target server

Identifying Name

____
Port number_______
OS _____________

Mouse settings *:
Acceleration______
Threshold_______

Target server

Identifying Name

____
Port number_______
OS _____________

Mouse settings *:
Acceleration______
Threshold_______

Target server

Identifying Name

____
Port number_______
OS _____________

Mouse settings *:
Acceleration______
Threshold_______

Target server

Identifying Name

____
Port number_______
OS _____________

Mouse settings *:
Acceleration______
Threshold_______

Target server

Identifying Name

____
Port number_______
OS _____________

Mouse settings *:
Acceleration______
Threshold_______

Target server

Identifying Name

____
Port number_______
OS _____________

Mouse settings *:
Acceleration______
Threshold_______

Target server

Identifying Name

____
Port number_______
OS _____________

Mouse settings *:
Acceleration______
Threshold_______

Target server

Identifying Name

____
Port number_______
OS _____________

Mouse settings *:
Acceleration______
Threshold_______

Target server

Identifying Name

____
Port number_______
OS _____________

Mouse settings *:
Acceleration______
Threshold_______

Target server

Identifying Name

____
Port number_______
OS _____________

Mouse settings *:
Acceleration______
Threshold_______

*** Only needed when not default**

MINICOM

advanced systems